

This Page Is Inserted by IFW Operations  
and is not a part of the Official Record

## **BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning documents *will not* correct images,  
please do not report the images to the  
Image Problem Mailbox.**

**THIS PAGE BLANK (USPTO)**

## PCT COOPERATION TREATY

PCT

## NOTIFICATION OF ELECTION

(PCT Rule 61.2)

From the INTERNATIONAL BUREAU

To:

United States Patent and Trademark  
Office  
(Box PCT)  
Crystal Plaza 2  
Washington, DC 20231  
ÉTATS-UNIS D'AMÉRIQUE

in its capacity as elected Office

<b>Date of mailing (day/month/year)</b> 16 March 1999 (16.03.99)	
<b>International application No.</b> PCT/EP98/04424	<b>Applicant's or agent's file reference</b> P96198WO/EK03
<b>International filing date (day/month/year)</b> 16 July 1998 (16.07.98)	<b>Priority date (day/month/year)</b> 06 August 1997 (06.08.97)
<b>Applicant</b> WILHELM, Siegfried et al	

1. The designated Office is hereby notified of its election made:



in the demand filed with the International Preliminary Examining Authority on:

03 March 1999 (03.03.99)



in a notice effecting later election filed with the International Bureau on:

2. The election ☒ was

was not

made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

<b>The International Bureau of WIPO</b> 34, chemin des Colombettes 1211 Geneva 20, Switzerland Facsimile No.: (41-22) 740.14.35	<b>Authorized officer</b>  Athina Nickitas-Etienne Telephone No.: (41-22) 338.83.38
--	--

**THIS PAGE BLANK (USPTO)**

Patent Claims

1. A decoder device having a control unit (RCU) for decrypting encrypted television programs, comprising
  - an input (4) for feeding in an encrypted television program;
  - a decryption device (DVB), which decrypts an encrypted television program into a format that can be reproduced by a television receiver (TV set);
  - an output (2), which can be connected to a television receiver (TV set) in order to feed the decrypted television program into the television receiver (TV set) for reproduction;
  - an interface (IFD 3,6) for an identification and/or key carrier component (ICC DVB) for enabling the decryption device (DVB); and
  - an interface (IR 3,6) for a control unit (RCU) of the decoder device (DVB);characterized in that
  - the interface (IFD 3,6) for the identification and/or key carrier component (ICC DVB) is arranged in the control unit (RCU) of the decoder device (STB).
2. The decoder device having a control unit (RCU) as recited in Claim 1, characterized in that
  - the control unit (RCU) is also set up for controlling the television receiver (TV set), which has an interface (IR (,9) [sic] for receiving control commands.
3. The decoder device having a control unit (RCU) as recited in Claim 1, characterized by
  - an interface (BC 5) to a telecommunications network.
4. The decoder device having a control unit (RCU) as recited in Claim 3, characterized by
  - an interface IFD (3,6) to an identification and/or

key carrier component (ICC BC), a connection being established via the telecommunications network to a specific subscriber as a function of an authorization by the identification and/or key carrier component (ICC BC).

5. The decoder device having a control unit (RCU) as recited in one of the preceding claims, characterized in that

- the interface to the identification and/or key carrier component for authorizing the connection via the telecommunications network is arranged in the control unit (RCU).

6. The decoder device having a control unit (RCU) as recited in one of the preceding claims, characterized in that

- the identification and/or key carrier component for authorizing the connection via the telecommunications network and the identification and/or key carrier component for enabling the encryption device are implemented either by two separate or by one common smart card.

7. The decoder device having a control unit (RCU) as recited in one of the preceding claims, characterized in that

- the decoder device has an interface (DVB) via which the decoder device can be connected to a computer (PC), which is set up for controlling the decoder device and/or for establishing a connection to another subscriber via the telecommunications network.

8. The decoder device having a control unit (RCU) as recited in one of the preceding claims, characterized in that

- the control unit (RCU) is made up of the computer (PC), which

- has an interface (IR 3, 7) for controlling the decoder device; and
- has an interface (IFD 3,6) for the identification and/or key carrier component (ICC BC) for authorizing the connection via the telecommunications network and/or the identification and/or key carrier component (ICC DVB) for enabling the decryption device (DVB).

9. The decoder device having a control unit (RCU) as recited in one of the preceding claims, characterized in that

- the decoder device is integrated in the television set.

10. A smart card for a decoder device having a control unit (RCU) as recited in one of the preceding claims, comprising

- a computer unit;
- a first memory area, in which are stored at least parts of operating system functions which are used to control the communication between the computer unit of the smart card and the peripherals of the smart card, as well as the communication with an external host computer, and which are used to manage protected, unprotected and/or read/write memory areas of the smart card;

and

- a second memory area, which is subdivided into protected and unprotected areas, access to protected areas being made as a function of a check for permitted access,

characterized in that

- a general key is stored in the protected area of the second memory area, and under the control of the general key, the external host computer enters at least one further simple key, as well as a protocol program associated with this further simple key.

11. The smart card as recited in Claim 10, characterized in that

- stored in the second memory area is a key management, from which access is made to a protocol program of a simple key.

12. A method for a host computer of a pay TV provider to communicate with a decoder device having a control unit (RCU) as recited in one of Claims 1 - 9, and a smart card according to one of Claims 10, 12, characterized by the following steps:

- a telecommunications connection is established by the host computer between the host computer and the decoder device with the control unit or the computer containing the control unit;
- the host computer checks the general key in the smart card;
- a simple key, as well as a protocol program associated with the key are communicated to the smart card in encrypted form, in the case that the check test has a positive result;
- the simple key and the protocol program associated with the key are entered into the protected memory area of the smart card;
- the protected memory area of the smart card is inhibited.

13. The method as recited in Claim 12, characterized in that

- before the simple key and the protocol program associated with the key are entered into the protected memory area of the smart card, the key and the protocol program are decrypted by the computer unit of the smart card.

14. The method as recited in Claim 12, characterized in



that some of the data transmission traffic is transmitted back and forth via interface (5) to the telephone network, and some via the line (1), together with or prior to the broadband, digitally encrypted pay TV useful signal, the information to be transmitted being distributed between the two channels in such a way that it is able to be decrypted only in an alternating and also only in a step-by-step manner, in each instance, with knowledge thereof.

## INTERNATIONALER RECHERCHENBERICHT

(Artikel 18 sowie Regeln 43 und 44 PCT)

Aktenzeichen des Anmelders oder Anwalts <b>P96198WO/EK03</b>	WEITERES VORGEHEN siehe Mitteilung über die Übermittlung des internationalen Recherchenberichts (Formblatt PCT/ISA/220) sowie, soweit zutreffend, nachstehender Punkt 5	
Internationales Aktenzeichen <b>PCT/EP 98/04424</b>	Internationales Anmeldedatum (Tag/Monat/Jahr) <b>16/07/1998</b>	(Frühestes) Prioritätsdatum (Tag/Monat/Jahr) <b>06/08/1997</b>
Anmelder <b>DEUTSCHE TELEKOM AG et al.</b>		

Dieser internationale Recherchenbericht wurde von der Internationalen Recherchenbehörde erstellt und wird dem Anmelder gemäß Artikel 18 übermittelt. Eine Kopie wird dem Internationalen Büro übermittelt.

Dieser internationale Recherchenbericht umfaßt insgesamt 3 Blätter.

☒ Darüber hinaus liegt ihm jeweils eine Kopie der in diesem Bericht genannten Unterlagen zum Stand der Technik bei.

1. ☐ Bestimmte Ansprüche haben sich als nichtrecherchierbar erwiesen (siehe Feld I).
2. ☐ Mangelnde Einheitlichkeit der Erfindung (siehe Feld II).
3. ☐ In der internationalen Anmeldung ist ein Protokoll einer Nucleotid- und/oder Aminosäuresequenz offenbart; die internationale Recherche wurde auf der Grundlage des Sequenzprotokolls durchgeführt.
  - ☐ das zusammen mit der internationalen Anmeldung eingereicht wurde.
  - ☐ das vom Anmelder getrennt von der internationalen Anmeldung vorgelegt wurde.
  - ☐ dem jedoch keine Erklärung beigelegt war, daß der Inhalt des Protokolls nicht über den Offenbarungsgehalt der internationalen Anmeldung in der eingereichten Fassung hinausgeht.
  - ☐ das von der Internationalen Recherchenbehörde in die ordnungsgemäße Form übertragen wurde.
4. Hinsichtlich der Bezeichnung der Erfindung
  - ☒ wird der vom Anmelder eingereichte Wortlaut genehmigt.
  - ☐ wurde der Wortlaut von der Behörde wie folgt festgesetzt.
5. Hinsichtlich der Zusammenfassung
  - ☒ wird der vom Anmelder eingereichte Wortlaut genehmigt.
  - ☐ wurde der Wortlaut nach Regel 38.2b) in der Feld III angegebenen Fassung von dieser Behörde festgesetzt. Der Anmelder kann der Internationalen Recherchenbehörde innerhalb eines Monats nach dem Datum der Absendung dieses internationalen Recherchenberichts eine Stellungnahme vorlegen.
6. Folgende Abbildung der Zeichnungen ist mit der Zusammenfassung zu veröffentlichen:
  - Abb. Nr. 2 ☒ wie vom Anmelder vorgeschlagen
  - ☐ weil der Anmelder selbst keine Abbildung vorgeschlagen hat.
  - ☐ weil diese Abbildung die Erfindung besser kennzeichnet.
  - ☐ keine der Abb.

84179105317

Nach der internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

## B. RECHERCHIERTE GEBIETE

Recherchierte Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)

IPK 6 H04N

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

## C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
Y	WO 97 20431 A (THOMSON MULTIMEDIA SA ; VITO MARIO DE (FR); GREGOIRE LOUIS (FR)) 5. Juni 1997 <del>siehe Seite 5, Zeile 27</del> <del>Seite 7, Zeile 8</del> <i>see pg. 5, line 27-</i> <del>siehe Seite 12, Zeile 1</del> <del>Seite 23</del> <i>pg. 7, line 8; see pg.</i> <del>siehe Seite 16, Zeile 24</del> <del>Seite 19, Zeile 7</del> <i>12, line 1 - line 23</i> <del>siehe Abbildungen 1, 2, 4</del> <i>see pg. 16, line 24 -</i> <i>See drawings 1, 2 + 4</i> <i>pg. 19, line 7</i>	1-14
Y	WO 96 32702 A (SMART TV CO) 17. Oktober 1996 <del>siehe Seite 4, Zeile 11</del> <del>Seite 6, Zeile 13</del> <i>see pg. 4, line 11 -</i> <del>siehe Seite 8, Zeile 9</del> <del>Seite 31</del> <i>pg. 6, line 13</i> <del>siehe Abbildungen 1-6</del> <i>see pg. 8, line 9 - pg. 31;</i> <i>-/- see drawings 1-6</i>	1-14



Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen



Siehe Anhang Patentfamilie

\* Besondere Kategorien von angegebenen Veröffentlichungen :

"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderscher Tätigkeit beruhend betrachtet werden

"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderscher Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann nahelegend ist

"Z" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche

16. November 1998

Absenddatum des internationalen Recherchenberichts

26/11/1998

Name und Postanschrift der Internationalen Recherchenbehörde

Europäisches Patentamt, P.B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,  
Fax: (+31-70) 340-3016

Bevollmächtigter Beauftragter

Van der Zaal, R

Kategorie	Bezeichnung der Vorrichtung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	GB 2 304 217 A (GEN INFORMATION SYSTEMS LTD) 12. März 1997 <del>siehe Seite 5, Zeile 17 - Seite 7, Zeile 2</del> <i>See pg. 5, line 17 -</i> <del>siehe Seite 8, Zeile 8 - Zeile 13</del> <i>pg. 7, line 2; see</i> <del>siehe Seite 12, Zeile 3 - Seite 13, Zeile 14</del> <i>pg. 8, line 8 -</i> <del>siehe Abbildungen 2-4</del> <i>line 13, see pg. 12, line 3 -</i> <i>pg. 13, line 14; see drawings</i>	1-6,9
A	BUER M ET AL: "INTEGRATED SECURITY FOR DIGITAL VIDEO BROADCAST" IEEE TRANSACTIONS ON CONSUMER ELECTRONICS, Bd. 42, Nr. 3, August 1996, Seiten 500-503, XP000638531 <del>siehe Seite 501, linke Spalte, Zeile 6 -</del> <i>see pg. 501, left column,</i> <del>Seite 503, linke Spalte, Zeile 35</del> <i>line 6 - pg. 503, left</i>	10-14
A	DE 94 17 937 U (C.I.S. HOTEL COMMUNICATIONS GMBH) 27. April 1995 <del>siehe Seite 6, Zeile 21 - Seite 9, Zeile 18</del> <del>siehe Abbildungen 1-4</del>	1,2,6

WO						
WO 9720431	A	05-06-1997	FR	2741972 A	06-06-1997	
			EP	0864226 A	16-09-1998	
WO 9632702	A	17-10-1996	AU	5449796 A	30-10-1996	
			CA	2218067 A	17-10-1996	
GB 2304217	A	12-03-1997	AU	6706396 A	12-03-1997	
			WO	9707632 A	27-02-1997	
DE 9417937	U	16-03-1995	AT	169170 T	15-08-1998	
			DE	19520180 A	15-05-1996	
			DE	59503015 D	03-09-1998	
			WO	9615629 A	23-05-1996	
			EP	0791272 A	27-08-1997	

## INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference P96198WO/EK03	<b>FOR FURTHER ACTION</b> See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)	
International application No. PCT/EP98/04424	International filing date (day/month/year) 16 July 1998 (16.07.1998)	Priority date (day/month/year) 06 August 1997 (06.08.1997)
International Patent Classification (IPC) or national classification and IPC H04N 7/16		
Applicant DEUTSCHE TELEKOM AG		

<p>1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.</p> <p>2. This REPORT consists of a total of <u>5</u> sheets, including this cover sheet.</p> <p><input checked="" type="checkbox"/> This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).</p> <p>These annexes consist of a total of <u>5</u> sheets.</p>	
<p>3. This report contains indications relating to the following items:</p> <p>I <input checked="" type="checkbox"/> Basis of the report</p> <p>II <input type="checkbox"/> Priority</p> <p>III <input type="checkbox"/> Non-establishment of opinion with regard to novelty, inventive step and industrial applicability</p> <p>IV <input type="checkbox"/> Lack of unity of invention</p> <p>V <input checked="" type="checkbox"/> Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement</p> <p>VI <input type="checkbox"/> Certain documents cited</p> <p>VII <input checked="" type="checkbox"/> Certain defects in the international application</p> <p>VIII <input type="checkbox"/> Certain observations on the international application</p>	

Date of submission of the demand 03 February 1999 (03.02.1999)	Date of completion of this report 09 August 1999 (09.08.1999)
Name and mailing address of the IPEA/EP European Patent Office D-80298 Munich, Germany Facsimile No. 49-89-2399-4465	Authorized officer Telephone No. 49-89-2399-0

# I. Basis of the report

1. This report has been drawn on the basis of (Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments.):

- ☐ the international application as originally filed.
- ☒ the description. pages 1-13, as originally filed.  
pages \_\_\_\_\_, filed with the demand.  
pages \_\_\_\_\_, filed with the letter of \_\_\_\_\_  
pages \_\_\_\_\_, filed with the letter of \_\_\_\_\_
- ☒ the claims. Nos. \_\_\_\_\_, as originally filed.  
Nos. \_\_\_\_\_, as amended under Article 19.  
Nos. \_\_\_\_\_, filed with the demand.  
Nos. 1-12, filed with the letter of 23 June 1999 (23.06.1999)  
Nos. \_\_\_\_\_, filed with the letter of \_\_\_\_\_
- ☒ the drawings. sheets/fig 1/4-4/4, as originally filed.  
sheets/fig \_\_\_\_\_, filed with the demand.  
sheets/fig \_\_\_\_\_, filed with the letter of \_\_\_\_\_  
sheets/fig \_\_\_\_\_, filed with the letter of \_\_\_\_\_

2. The amendments have resulted in the cancellation of:

- ☐ the description. pages \_\_\_\_\_
- ☐ the claims. Nos. \_\_\_\_\_
- ☐ the drawings. sheets/fig \_\_\_\_\_

3. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).

4. Additional observations, if necessary:

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	1 - 12	YES
	Claims		NO
Inventive step (IS)	Claims	1 - 12	YES
	Claims		NO
Industrial applicability (IA)	Claims	1 - 12	YES
	Claims		NO

2. Citations and explanations

1. Reference is made to the following documents:

- D1: WO-A-97/20431  
D2: WO-A-96/32702  
D3: GB-A-2 304 217  
D4: DE-U-94 17 937  
D5: BUER M ET AL: "INTEGRATED SECURITY FOR DIGITAL VIDEO BROADCAST", IEEE TRANSACTIONS ON CONSUMER ELECTRONICS, Vol. 42, No. 3, August 1996, pages 500 - 503

2. Document D1 discloses a transcoder provided with an control unit and intended for decoding encoded TV programs according to the preamble of Claim 1.

The subject matter of Claim 1 is distinguished from the above-mentioned prior art in that the interface for the identification carrier component is arranged in the control unit and in that the establishment of a connection via the telecommunication network is dependent on an authorization by the identification carrier component. Independent Claims 8 and 10 relate to a chip card for a transcoder according to Claim 1 and a method for the communication of a host

.../...



computer of a pay TV provider with a transcoder and a chip card according to Claims 1 and 8.

The other documents cited in the international search report are less relevant to the subject matter of the application. Documents D2 - D4 do not relate to transcoders for decoding encoded TV programs. In document D5, the identification carrier component is integrated in the transcoder.

Consequently, the transcoder, the chip card and the method according to Claims 1, 8 and 10 are neither known from, nor suggested by, the known prior art. Claims 1, 8 and 10 therefore comply with the requirements of PCT Article 33(2) and (3).

3. Dependent Claims 2 - 7, 9, 11 and 12 relate to advantageous embodiments of the subjects of Claims 1, 8 and 10 and therefore they, too, comply with the requirements of PCT Article 33(2) and (3).

**VII. Certain defects in the international application**

The following defects in the form or contents of the international application have been noted:

1. The description did not cite documents D1 and D2 and did not indicate the relevant prior art disclosed therein, in contravention of the requirements of PCT Rule 5.1(a)(ii).
2. The description is not in line with the claims, contrary to PCT Rule 5.1(a)(iii).

From the  
INTERNATIONAL PRELIMINARY EXAMINING AUTHORITY

To:

WUESTHOFF & WUESTHOFF  
Schweigerstrasse 4  
D-81541 Munich  
GERMANY

[stamp]

**PCT**

**NOTIFICATION OF TRANSMITTAL OF  
INTERNATIONAL PRELIMINARY  
EXAMINATION REPORT**

(PCT Rule 71.1)

Date of mailing (day/month/year)  
09.08.99

Applicant's or agent's file reference  
P96198WO/EK03

**IMPORTANT NOTIFICATION**

International application No.  
PCT/EP98/04424

International filing date (day/month/year)  
16/07/1998

Priority date (day/month/year)  
06/08/1997

Applicant  
DEUTSCHE TELEKOM AG et al.

1. The applicant is hereby notified that this International Preliminary Examining Authority transmits herewith the international preliminary examination report and its annexes, if any, established on the international application.
2. A copy of the report and its annexes, if any, is being transmitted to the International Bureau for communication to all the elected Offices.
3. Where required by any of the elected Offices, the International Bureau will prepare an English translation of the report (but not of any annexes) and will transmit such translation to those Offices.
4. REMINDER

The applicant must enter the national phase before each elected Office by performing certain acts (filing translations and paying national fees) within 30 months from the priority date (or later in some Offices) (Article 39(1)) (see also the reminder sent by the International Bureau with Form PCT/IB/301).

Where a translation of the international application must be furnished to an elected Office, that translation must contain a translation of any annexes to the International preliminary examination report. It is the applicant's responsibility to prepare and furnish such translation directly to each elected Office concerned.

For further details on the applicable time limits and requirements of the elected Offices, see Volume II of the PCT Applicant's Guide.

Name and mailing address of the IPEA/



European Patent Office  
D-80298 Munich  
Tel. (+ 49-89) 2399-0, Tx: 523656 epmu d  
Fax: (+ 49-89) 2399-4465

Authorized officer:



Stannartz, B  
Tel. (+49-89) 2399-8242

8 L 179 105 317

## PATENT COOPERATION TREATY

## PCT



## INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or Agent's file reference P96198WO/EK03	<b>FOR FURTHER ACTION</b>		See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
International application No. PCT/EP98/04424	International filing date (day/month/year) 16/07/1998	Priority date (day/month/year) 06/08/1997	
International Patent Classification (IPC) or national classification and IPC H04N7/16			
Applicant DEUTSCHE TELEKOM AG et al.			

1. This internal preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.
2. This REPORT consists of a total of 5 sheets including this title page.
- ☒ This report is also accompanied by ANNEXES, i.e. sheets of the description, claims and/or drawings amended during international preliminary examination and/or containing rectifications made before this Authority (see Rule 70.16 and Instruction 607 of PCT Administrative Instructions).
- These annexes consist of a total of 5 sheets.

3. This report contains indications relating to the following items:
- I ☒ Basis of the report
  - II ☐ Priority
  - III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
  - IV ☐ Lack of unity of invention
  - V ☒ Reasoned statement according to Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
  - VI ☐ Certain documents cited
  - VII ☒ Certain defects in the international application
  - VIII ☐ Certain observations on the international application

Date of submission of the demand 03/02/1999	Date of completion of this report 09.08.99
<b>Name and mailing address of the IPEA/</b>   European Patent Office D-80298 Munich Tel. (+ 49-89) 2399-0, Tx: 523656 epmu d Fax: (+ 49-89) 2399-4465	<b>Authorized officer:</b>  Schinnerl, A  Telephone No. (+49-89) 2399 

**I. Basis of the report**

1. This report has been drawn up on the basis of the following elements *(the replacement sheets received by the receiving office in response to an invitation according to Article 14 are considered in the present report as "originally filed" and are not annexed to the report as they contain no amendments.)*:

**Description, pages:**

1-13 as originally filed

**Claims, No.:**

1-12 received on 23/06/1999 with the letter of 23/06/1999

**Drawings, sheets:**

1/4-4/4 as originally filed

2. The amendments have resulted in the cancellation of:

☐ the description, pages:

☐ the claims, Nos.:

☐ the drawings, sheets:

3. ☐ The present report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated as follows (Rule 70.2(c)):

4. Additional observations, if necessary:

**V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement****1. Statement**

Novelty	Yes:	Claims	1-12
	No:	Claims	
Inventive Step	Yes:	Claims	1-12
	No:	Claims	
Industrial Applicability	Yes:	Claims	1-12
	No:	Claims	

**2. Citations and explanations****see separate sheet****VII. Certain defects in the international application**

The following defects in the form or contents of the international application have been noted:

**see separate sheet**

Re Point V

V. Reasoned statement under Rule 66.2(s)(ii) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Reference is made to the following documents:

D1: WO-A-97 20431

D2: WO-A-96 32702

D3: GB-A-2 304 217

D4: DE-U-94 17 937

D5: BUER M ET AL: "INTEGRATED SECURITY FOR DIGITAL VIDEO BROADCAST", IEEE TRANSACTIONS ON CONSUMER ELECTRONICS, Vol. 42, No. 3, August 1996, pages 500-503

2. Document D1 discloses a decoder device with a control unit for decrypting encrypted television programs in accordance with the preamble of Claim 1.

The subject matter of Claim 1 differs from the abovementioned prior art by virtue of the fact that the interface for the identification carrier component is arranged in the control unit, and that a connection via the telecommunications network is established in a manner dependent on authorization by the identification carrier component. The independent Claims 8 and 10 relate to a smart card for a decoder device according to Claim 1 and a method for the communication of a host computer of a Pay TV provider with a decoder device and a smart card according to Claims 1 and 8.

The further documents cited in the international search report are connected with the subject matter of the application to a lesser extent. Documents D2-D4 do not relate to decoder devices for decrypting encrypted television programs. In document D5, the identification carrier component is integrated in the decoder device.

Therefore, the decoder device, the smart card and the method in accordance with Claims 1, 8 and 10 are neither disclosed in the known prior art nor suggested by it. Consequently, Claims 1, 8 and 10 fulfill the requirements of Article 33(2) and (3) PCT.

3. The dependent Claims 2-7, 9, 11 and 12 relate to advantageous refinements of the subject-matters of Claims 1, 8 and 10 and therefore, they, too, fulfill the requirements of Article 33(2) and (3) PCT.

#### Re Point VII

##### **Certain defects in the international application**

1. Contrary to the requirements of rule 5.1 a)ii) PCT, neither the relevant prior art disclosed in documents D1 and D2 nor these documents are specified in the description.
2. Contrary to the prescription in rule 5.1 a)iii) PCT, the description does not correspond to the claims.



## INTERNATIONAL PRELIMINARY

EXAMINATION REPORT International application No. PCT/EP98/04424

---

**I. Basis of the report**

1. This report has been drawn up on the basis of the following elements (the replacement sheets received by the receiving office in response to an invitation according to Article 14 are considered in the present report as "originally filed" and are not annexed to the report as they contain no amendments.):

**Description, pages:**

1-13 as originally filed

**Claims, No.:**

1-12 received on 23/06/1999 with the letter of  
23/06/1999

**Drawings, sheets:**

1/4-4/4 as originally filed

2. The amendments have resulted in the cancellation of:

☐ the description, pages:

☐ the claims, Nos.:

☐ the drawings, sheets:

3. ☐ The present report has been established as if

NY01 249126 v 1

24179105 317

(some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated as follows (Rule 70.2(c)):

4. Additional observations, if necessary:

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty	Yes:	Claims	1-12
	No:	Claims	

Inventive Step	Yes:	Claims	1-12
	No:	Claims	

Industrial Applicability	Yes:	Claims	1-12
	No:	Claims	

2. Citations and explanations

see separate sheet

#### VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

see separate sheet

Re Point V

V. Reasoned statement under Rule 66.2 (s) (ii) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Reference is made to the following documents:

D1: WO-A-97 20431  
D2: WO-A-96 32702  
D3: GB-A-2 304 217  
D4: DE-U-94 17 937  
D5: BUER M ET AL: "INTEGRATED SECURITY  
FOR  
DIGITAL VIDEO BROADCAST-, IEEE  
TRANSACTIONS  
ON CONSUMER ELECTRONICS, Vol. 42, No.  
3,  
August 1996, pages 500-503

2. Document D1 discloses a decoder device with a control unit for decrypting encrypted television programs in accordance with the preamble of Claim 1.

The subject matter of Claim 1 differs from the abovementioned prior art by virtue of the fact that the interface for the identification carrier component is arranged in the control unit, and that a connection via the telecommunications network is established in a manner dependent on authorization by the identification carrier component. The independent

Claims 8 and 10 relate to a smart card for a decoder device according to Claim 1 and a method for the communication of a host computer of a Pay TV provider with a decoder device and a smart card according to Claims 1 and 8.

The further documents cited in the international search report are connected with the subject matter of the application to a lesser extent. Documents D2-D4 do not relate to decoder devices for decrypting encrypted television programs. In document D5, the identification carrier component is integrated in the decoder device.

Therefore, the decoder device, the smart card and the method in accordance with Claims 1, 8 and 10 are neither disclosed in the known prior art nor suggested by it. Consequently, Claims 1, 8 and 10 fulfill the requirements of Article 33(2) and (3) PCT.

3. The dependent Claims 2-7, 9, 11 and 12 relate to advantageous refinements of the subject-matters of Claims 1, 8 and 10 and therefore, they, too, fulfill the requirements of Article 33(2) and (3) PCT.

#### Re Point VII

##### **Certain defects in the international application**

1. Contrary to the requirements of rule 5.1 a)ii) PCT, neither the relevant prior art disclosed in documents D1 and D2 nor these documents are specified in the description.
2. Contrary to the prescription in rule 5.1 a)iii) PCT, the description does not correspond to the claims.

## Claims

1. Decoder device (STB) with a control unit (RCU), for  
5 the decryption of encrypted television programs, having  
- an input (4) for feeding in an encrypted television  
program,  
- a decryption device (DVB), which decrypts an  
10 encrypted television program into a format that be  
reproduced by means of a television receiver (TV),  
- an output (2), which can be connected to a  
television receiver (TV) in order to feed the decrypted  
television program into the television receiver (TV) for  
reproduction,  
15 - an interface (IFD 3,6) for an identification  
and/or key carrier component (ICC DVB) for enabling the  
decryption device (DVB), an interface (IR 3,6) for a  
control unit (RCU) of the decoder device (STB), and an  
interface (BC 5) to a telecommunications network (Tel.  
20 Network),  
characterized in that  
- the interface (IFD 3,6) for the identification  
and/or key carrier components (ICC DVB) is arranged in  
the control unit (RCU) of the decoder device (STB), and  
25 - an interface IFD (3,6) to an identification and/or  
key carrier component (ICC BC), a connection via the  
telecommunications network (Tel. Network) to a specific  
subscriber being established in a manner dependent on  
authorization by the identification and/or key carrier  
30 component (ICC BC) is present.
2. Decoder device with a control unit (RCU) according  
to Claim 1, characterized in that  
- the interface (IFD 3,6) to the identification and/or  
35 key carrier component for the authorization of the  
connection via the telecommunications network is arranged  
in the control unit (RCU).

3. Decoder device (STB) with a control unit (RCU) according to Claim 1 or 2, characterized in that  
- the control unit (RCU) is also set up for controlling the television receiver (TV Set) , which has an interface (IR 9) for receiving control commands.

4. Decoder device (STB) with a control unit (RCU) according to one of the preceding claims, characterized in that the identification and/or key carrier component (ICC BC) for the authorization of the connection via the telecommunications network (Tel. Network) and the identification and/or key carrier component (ICC BVB) for enabling the encryption device (DVB) are realized either by two separate or by one common smart card.

5. Decoder device (STB) with a control unit (RCU) according to one of the preceding claims, characterized in that  
- the decoder device (STB) has an interface (PCI) via which the decoder device (STB) can be connected to a computer (PC), which is set up for controlling the decoder device (STB) and/or for establishing a connection to another subscriber via the telecommunications network (Tel. Network).

6. Decoder device (STB) with a control unit (RCU) according to one of the preceding claims, characterized in that  
- the control unit (RCU) is formed by the computer (PC), which  
- has an interface (R 3,6,7) in order to control the decoder device (STB), and  
- has an interface (IFD 3,6) for the identification and/or key carrier component (ICC BC) for the authorization of the connection via the telecommunications network (Tel. Network) and/or the identification and/or key carrier component (ICC DVB) for

enabling the decryption device (DVB).

7. Decoder device (STB) with a control unit (RCU) according to one of the preceding claims, characterized in that

- the decoder device (STB) is integrated in the television set (TV).

8. Smart card for a decoder device with a control unit (RCU) according to one of the preceding claims, having

- a computer unit,  
- a first memory area, in which there are stored at least parts of operating system functions with which the communication between the computer unit of the smart card and the peripherals of the smart card, and also the communication with an external host computer are controlled, and with which protected, unprotected and/or read/write memory areas of the smart card are managed, and

- a second memory area, which is subdivided into protected and unprotected areas, access to protected areas being made depending on a result of a check of the admissibility of the access, characterized in that

- a general key is stored in the protected area of the second memory area, and the entry of at least one further simple key and also of a protocol program associated with this further simple key by the external host computer being effected under the control of said general key.

9. Smart card according to Claim 10 [sic], characterized in that

- a key management is stored in the second memory area and from it access is made to a protocol program of a simple key.

10. Method for the communication of a host computer of a

Pay TV provider with a decoder device with a control unit (RCU) according to one of Claims 1 - 7 and a smart card according to Claim 8 or 9, characterized by the following steps:

- 5       - establishment of a telecommunications connection between the host computer and the decoder device with the control unit or the computer containing the control unit by the host computer,
- checking of the general key in the smart card by the  
10       host computer,
- communication of a simple key and also of a protocol program associated with said key to the smart card in encrypted form, if the check has a positive result,
- entry of the simple key and also of the protocol  
15       program associated with said key into the protected memory area of the smart card,
- inhibiting of the protected memory area of the smart card.

- 20       11. Method according to Claim 10, characterized in that
- before the entry of the simple key and also of the protocol program associated with said key into the protected memory area of the smart card, the key and the protocol program are preferably decrypted by the computer  
25       unit of the smart card.

12. Method according to Claim 10, characterized in that a portion of the data transmission traffic is transmitted back and forth via the interface (5) to the telephone  
30       network and a further portion via a line (1); which is connected to the television set (TV) for the purpose of transmitting the encrypted television program, with or before a useful signal that reproduces the encrypted television program, the information to be transmitted  
35       being subdivided and transmitted in such a way that it can be decrypted only in an alternating manner and also only in a step-by-step manner with respective knowledge.






PCT

REC'D 11 AUG 1999

WIPO PCT

# INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

(Artikel 36 und Regel 70 PCT)

Aktenzeichen des Anmelders oder Anwalts <b>P96198WO/EK03</b>		WEITERES VORGEHEN siehe Mitteilung über die Übersendung des internationalen vorläufigen Prüfungsbericht (Formblatt PCT/IPEA/416)	
Internationales Aktenzeichen <b>PCT/EP98/04424</b>	Internationales Anmeldedatum (Tag/Monat/Jahr) <b>16/07/1998</b>	Prioritätsdatum (Tag/Monat/Jahr) <b>06/08/1997</b>	
Internationale Patentklassifikation (IPK) oder nationale Klassifikation und IPK <b>H04N7/16</b>			
Anmelder <b>DEUTSCHE TELEKOM AG et al.</b>			
1. Dieser internationale vorläufige Prüfungsbericht wurde von der mit der internationale vorläufigen Prüfung beauftragte Behörde erstellt und wird dem Anmelder gemäß Artikel 36 übermittelt.  2. Dieser BERICHT umfaßt insgesamt 5 Blätter einschließlich dieses Deckblatts.  <input checked="" type="checkbox"/> Außerdem liegen dem Bericht ANLAGEN bei; dabei handelt es sich um Blätter mit Beschreibungen, Ansprüchen und/oder Zeichnungen, die geändert wurden und diesem Bericht zugrunde liegen, und/oder Blätter mit vor dieser Behörde vorgenommenen Berichtigungen (siehe Regel 70.16 und Abschnitt 607 der Verwaltungsrichtlinien zum PCT).  Diese Anlagen umfassen insgesamt 5 Blätter.			
3. Dieser Bericht enthält Angaben zu folgenden Punkten:  I <input checked="" type="checkbox"/> Grundlage des Berichts II <input type="checkbox"/> Priorität III <input type="checkbox"/> Keine Erstellung eines Gutachtens über Neuheit, erfinderische Tätigkeit und gewerbliche Anwendbarkeit IV <input type="checkbox"/> Mangelnde Einheitlichkeit der Erfindung V <input checked="" type="checkbox"/> Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderische Tätigkeit und der gewerbliche Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung VI <input type="checkbox"/> Bestimmte angeführte Unterlagen VII <input checked="" type="checkbox"/> Bestimmte Mängel der internationalen Anmeldung VIII <input type="checkbox"/> Bestimmte Bemerkungen zur internationalen Anmeldung			
Datum der Einreichung des Antrags  <b>03/02/1999</b>		Datum der Fertigstellung dieses Berichts  <b>09. 08. 99</b>	
Name und Postanschrift der mit der internationalen vorläufigen Prüfung beauftragten Behörde:   Europäisches Patentamt D-80298 München Tel. (+49-89) 2399-0 Tx: 523656 epmu d Fax: (+49-89) 2399-4465		Bevollmächtigter Bediensteter  <b>Schinnerl, A</b>  Tel. Nr. (+49-89) 2399	




PCT

REC'D 11 AUG 1999

WIPO PCT

## INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

(Artikel 36 und Regel 70 PCT)

Aktenzeichen des Anmelders oder Anwalts P96198WO/EK03	<b>WEITERES VORGEHEN</b> siehe Mitteilung über die Übersendung des internationalen vorläufigen Prüfungsbericht (Formblatt PCT/IPEA/416)	
Internationales Aktenzeichen PCT/EP98/04424	Internationales Anmeldedatum (Tag/Monat/Jahr) 16/07/1998	Prioritätsdatum (Tag/Monat/Jahr) 06/08/1997
Internationale Patentklassifikation (IPK) oder nationale Klassifikation und IPK H04N7/16		
Anmelder DEUTSCHE TELEKOM AG et al.		
<p>1. Dieser internationale vorläufige Prüfungsbericht wurde von der mit der internationale vorläufigen Prüfung beauftragte Behörde erstellt und wird dem Anmelder gemäß Artikel 36 übermittelt.</p> <p>2. Dieser BERICHT umfaßt insgesamt 5 Blätter einschließlich dieses Deckblatts.</p> <p><input checked="" type="checkbox"/> Außerdem liegen dem Bericht ANLAGEN bei; dabei handelt es sich um Blätter mit Beschreibungen, Ansprüchen und/oder Zeichnungen, die geändert wurden und diesem Bericht zugrunde liegen, und/oder Blätter mit vor dieser Behörde vorgenommenen Berichtigungen (siehe Regel 70.16 und Abschnitt 607 der Verwaltungsrichtlinien zum PCT).</p> <p>Diese Anlagen umfassen insgesamt 5 Blätter.</p>		
<p>3. Dieser Bericht enthält Angaben zu folgenden Punkten:</p> <p>I <input checked="" type="checkbox"/> Grundlage des Berichts</p> <p>II <input type="checkbox"/> Priorität</p> <p>III <input type="checkbox"/> Keine Erstellung eines Gutachtens über Neuheit, erfinderische Tätigkeit und gewerbliche Anwendbarkeit</p> <p>IV <input type="checkbox"/> Mangelnde Einheitlichkeit der Erfindung</p> <p>V <input checked="" type="checkbox"/> Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderische Tätigkeit und der gewerbliche Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung</p> <p>VI <input type="checkbox"/> Bestimmte angeführte Unterlagen</p> <p>VII <input checked="" type="checkbox"/> Bestimmte Mängel der internationalen Anmeldung</p> <p>VIII <input type="checkbox"/> Bestimmte Bemerkungen zur internationalen Anmeldung</p>		
Datum der Einreichung des Antrags  03/02/1999	Datum der Fertigstellung dieses Berichts  09.08.99	
Name und Postanschrift der mit der internationalen vorläufigen Prüfung beauftragten Behörde:   Europäisches Patentamt D-80298 München Tel. (+49-89) 2399-0 Tx: 523656 epmu d Fax: (+49-89) 2399-4465	Bevollmächtigter Bediensteter  Schinnerl, A  Tel. Nr. (+49-89) 2399	



**I. Grundlage des Berichts**

1. Dieser Bericht wurde erstellt auf der Grundlage (*Ersatzblätter, die dem Anmeldeamt auf eine Aufforderung nach Artikel 14 hin vorgelegt wurden, gelten im Rahmen dieses Berichts als "ursprünglich eingereicht" und sind ihm nicht beigelegt, weil sie keine Änderungen enthalten.*):

**Beschreibung, Seiten:**

1-13 ursprüngliche Fassung

**Patentansprüche, Nr.:**

1-12 eingegangen am 23/06/1999 mit Schreiben vom 23/06/1999

**Zeichnungen, Blätter:**

1/4-4/4 ursprüngliche Fassung

2. Aufgrund der Änderungen sind folgende Unterlagen fortgefallen:

- ☐ Beschreibung, Seiten:  
☐ Ansprüche, Nr.:  
☐ Zeichnungen, Blatt:

3. ☐ Dieser Bericht ist ohne Berücksichtigung (von einigen) der Änderungen erstellt worden, da diese aus den angegebenen Gründen nach Auffassung der Behörde über den Offenbarungsgehalt in der ursprünglich eingereichten Fassung hinausgehen (Regel 70.2(c)):

4. Etwaige zusätzliche Bemerkungen:

**V. Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung**

**1. Feststellung**

Neuheit (N)	Ja: Ansprüche 1-12 Nein: Ansprüche
Erfinderische Tätigkeit (ET)	Ja: Ansprüche 1-12 Nein: Ansprüche
Gewerbliche Anwendbarkeit (GA)	Ja: Ansprüche 1-12 Nein: Ansprüche

2. Unterlagen und Erklärungen

**siehe Beiblatt**

**VII. Bestimmte Mängel der internationalen Anmeldung**

Es wurde festgestellt, daß die internationale Anmeldung nach Form oder Inhalt folgende Mängel aufweist:

**siehe Beiblatt**

Zu Punkt V

**Begründete Feststellung nach Regel 66.2(a)(ii) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung**

1. Es wird auf die folgenden Dokumente verwiesen:

D1: WO-A-97 20431

D2: WO-A-96 32702

D3: GB-A-2 304 217

D4: DE-U-94 17 937

D5: BUER M ET AL: "INTEGRATED SECURITY FOR DIGITAL VIDEO BROADCAST", IEEE TRANSACTIONS ON CONSUMER ELECTRONICS, Bd. 42, Nr. 3, August 1996, Seiten 500-503

2. Dokument D1 offenbart eine Decoder-Einrichtung mit einer Bedienungseinheit für die Entschlüsselung von verschlüsselten Fernsehprogrammen gemäß dem Oberbegriff des Anspruchs 1.

Der Gegenstand des Anspruchs 1 unterscheidet sich vom oben genannten Stand der Technik dadurch, daß die Schnittstelle für das Identifikationsträgerbauteil in der Bedienungseinheit angeordnet ist und daß die Herstellung einer Verbindung über das Telekommunikationsnetz abhängig von einer Autorisierung durch das Identifikationsträgerbauteil erfolgt. Die unabhängigen Ansprüche 8 und 10 betreffen eine Chip-Karte für eine Decoder-Einrichtung nach Anspruch 1 und ein Verfahren zur Kommunikation eines Host-Rechners eines Pay-TV-Anbieters mit einer Decoder-Einrichtung und einer Chip-karte nach den Ansprüchen 1 und 8.

Die weiteren im Internationalen Recherchenbericht genannten Dokumente stehen dem Anmeldungsgegenstand ferner. Die Dokumente D2-D4 betreffen keine Decoder-Einrichtungen zum Entschlüsseln von verschlüsselten

Fernsehprogrammen. In Dokument D5 ist der Identifikationsträgerbauteil in der Decoder-Einrichtung integriert.

Daher sind die Decoder-Einrichtung, die Chip-Karte und das Verfahren gemäß der Ansprüche 1, 8 und 10 aus dem bekannten Stand der Technik weder bekannt noch durch ihn nahegelegt. Die Ansprüche 1, 8 und 10 erfüllen somit die Erfordernisse des Artikels 33(2) und (3) PCT.

3. Die abhängigen Ansprüche 2-7, 9, 11 und 12 betreffen vorteilhafte Ausgestaltungen der Gegenstände der Ansprüche 1, 8 und 10, und daher erfüllen auch sie die Erfordernisse des Artikels 33(2) und (3) PCT.

#### **Zu Punkt VII**

#### **Bestimmte Mängel der internationalen Anmeldung**

1. Im Widerspruch zu den Erfordernissen der Regel 5.1 a) ii) PCT werden in der Beschreibung weder der in den Dokumenten D1 und D2 offenbarte einschlägige Stand der Technik noch diese Dokumente angegeben.
2. Die Beschreibung steht nicht, wie in Regel 5.1 a) iii) PCT vorgeschrieben, in Einklang mit den Ansprüchen.

## Ansprüche

1. Decoder-Einrichtung (STB) mit einer Bedienungseinheit (RCU), für die Entschlüsselung von verschlüsselten Fernseh-  
5 Programmen, mit
  - einem Eingang (4) zum Einspeisen eines verschlüsselten Fernseh-Programmes,
  - einer Entschlüsselungseinrichtung (DVB), die ein verschlüsseltes Fernseh-Programm in ein mittels eines Fernsehgeräts (TV)  
10 wiedergegbares Format entschlüsselt,
    - einem Ausgang (2), der mit einem Fernsehgerät (TV) verbindbar ist, um das entschlüsselte Fernseh-Programm in das Fernsehgerät (TV) zur Wiedergabe einzuspeisen,
    - einer Schnittstelle (IFD 3,6) für ein Identifikations-  
15 und/oder Schlüsselträgerbauteil (ICC DVB) zur Freigabe der Entschlüsselungseinrichtung (DVB),
    - einer Schnittstelle (IR 3,6) für eine Bedienungseinheit (RCU) der Decoder-Einrichtung (STB), und
    - einer Schnittstelle (BC 5) zu einem Telekommunikationsnetz  
20 (Tel. Netz),
- dadurch gekennzeichnet, daß
  - die Schnittstelle (IFD 3,6) für das Identifikations- und/oder Schlüsselträgerbauteil (ICC DVB) in der Bedienungseinheit (RCU) der Decoder-Einrichtung (STB) angeordnet ist, und  
25 - eine Schnittstelle (IFD 3,6) zu einem Identifikations- und/oder Schlüsselträgerbauteil (ICC BC) vorhanden ist, wobei die Herstellung einer Verbindung über das Telekommunikations-  
netz (Tel. Netz) mit einem bestimmten Teilnehmer abhängig von einer Autorisierung durch das Identifikations- und/oder Schlüs-  
30 selträgerbauteil (ICC BC) erfolgt.
2. Decoder-Einrichtung mit einer Bedienungseinheit (RCU) nach Anspruch 1, dadurch gekennzeichnet, daß
  - die Schnittstelle (IFD 3,6) zu dem Identifikations- und/oder  
35 Schlüsselträgerbauteil (ICC BC) für die Autorisierung der Ver-

GEÄNDERTES BLATT



bindung über das Telekommunikationsnetz (Tel. Netz) in der Bedienungseinheit (RCU) angeordnet ist.

3. Decoder-Einrichtung (STB) mit einer Bedienungseinheit (RCU) nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß  
5 - die Bedienungseinheit (RCU) auch zur Bedienung des Fernseh-Empfängers (TV Set) eingerichtet ist, der eine Schnittstelle (IR 9) zum Empfang von Steuerbefehlen aufweist.
- 10 4. Decoder-Einrichtung (STB) mit einer Bedienungseinheit (RCU) nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß  
- das Identifikations- und/oder Schlüsselträgerbauteil (ICC BC) für die Autorisierung der Verbindung über das Telekommunikationsnetz (Tel. Netz) und das Identifikations- und/oder Schlüsselträgerbauteil (ICC BVB) zur Freigabe der Entschlüsselungseinrichtung (DVB) entweder durch zwei getrennte oder durch eine gemeinsame Chip-Karte realisiert sind.
- 15 5. Decoder-Einrichtung (STB) mit einer Bedienungseinheit (RCU) nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß  
- die Decoder-Einrichtung (STB) eine Schnittstelle (PCI) aufweist, über die die Decoder-Einrichtung (STB) mit einem Rechner (PC) verbindbar ist, der zur Steuerung der Decoder-Einrichtung (STB) und/oder zur Herstellung einer Verbindung mit einem anderen Teilnehmer über das Telekommunikationsnetz (Tel. Netz) eingerichtet ist.
- 20 6. Decoder-Einrichtung (STB) mit einer Bedienungseinheit (RCU) nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß  
- die Bedienungseinheit (RCU) durch den Rechner (PC) gebildet ist, der
- 25 30

GEÄNDERTES BLATT

- eine Schnittstelle (IR 3,6,7) aufweist, um die Decoder-Einrichtung (STB) zu steuern, und
  - eine Schnittstelle (IFD 3,6) für das Identifikations- und/oder Schlüsselträgerbauteil (ICC BC) für die Autorisierung
- 5 der Verbindung über das Telekommunikationsnetz (Tel. Netz) bzw. das Identifikations- und/oder Schlüsselträgerbauteil (ICC DVB) zur Freigabe der Entschlüsselungseinrichtung (DVB) aufweist.

7. Decoder-Einrichtung (STB) mit einer Bedienungseinheit
- 10 (RCU) nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß
- die Decoder-Einrichtung (STB) in das Fernsehgerät (TV) integriert ist.

- 15 8. Chip-Karte für eine Decoder-Einrichtung mit einer Bedienungseinheit (RCU) nach einem der vorhergehenden Ansprüche, mit
- einer Rechneinheit,
  - einem ersten Speicherbereich, in dem zumindest Teile von Betriebssystem-Funktionen abgelegt sind, mit denen die Kommunikation
- 20 zwischen der Rechneinheit der Chip-Karte und den Peripherie-Geräten der Chip-Karte, sowie die Kommunikation mit einem externen Host-Rechner gesteuert wird, und mit denen geschützte, ungeschützte, und/oder Schreib/Lese-Speicher-Bereiche der Chip-Karte verwaltet werden, und
- 25 - einem zweiten Speicherbereich, der in geschützte und ungeschützte Bereiche unterteilt ist, wobei der Zugriff auf geschützte Bereiche in Abhängigkeit von einem Ergebnis einer Überprüfung der Zulässigkeit des Zugriffs erfolgt, dadurch gekennzeichnet, daß
- 30 - in dem geschützten Bereich des zweiten Speicherbereiches ein Generalschlüssel abgelegt ist, unter dessen Kontrolle die Eintragung wenigstens eines weiteren einfachen Schlüssels sowie eines zu diesem weiteren einfachen Schlüssel gehörendes Protokoll-Programm durch den externen Host-Rechner erfolgt.

9. Chip-Karte nach Anspruch 10, dadurch gekennzeichnet, daß  
- in dem zweiten Speicherbereich eine Schlüssel-Verwaltung ab-  
gelegt ist, von der aus der Zugriff auf ein Protokoll-Programm  
eines einfachen Schlüssels erfolgt.

5

10. Verfahren zur Kommunikation eines Host-Rechners eines Pay-  
TV-Anbieters mit einer Decoder-Einrichtung mit einer Bedie-  
nungseinheit (RCU) nach einem der Ansprüche 1 - 7, und einer  
Chip-Karte nach Anspruch 8 oder 9 gekennzeichnet durch folgende

10 Schritte:

- Herstellen einer Telekommunikationsverbindung zwischen dem  
Host-Rechner und der Decoder-Einrichtung mit der Bedienungsein-  
heit oder dem die Bedienungseinheit enthaltenden Rechner durch  
den Host-Rechner,

15 - Überprüfen des Generalschlüssels in der Chip-Karte durch den  
Host-Rechner,

- Übermitteln eines einfachen Schlüssels sowie eines zu diesem  
Schlüssel gehörenden Protokoll-Programmes an die Chip-Karte in  
verschlüsselter Form, falls die Überprüfung positiv ausfällt,

20 - Eintragen des einfachen Schlüssels sowie des zu diesem  
Schlüssel gehörenden Protokoll-Programmes in den geschützten  
Speicherbereich der Chip-Karte,

- Sperren des geschützten Speicherbereiches der Chip-Karte.

25 11. Verfahren nach Anspruch 10, dadurch gekennzeichnet, daß  
- vor dem Eintragen des einfachen Schlüssels sowie des zu die-  
sem Schlüssel gehörenden Protokoll-Programmes in den geschütz-  
ten Speicherbereich der Chip-Karte der Schlüssel und das Proto-  
koll-Programm vorzugsweise durch die Rechneinheit der Chip-  
30 karte entschlüsselt werden.

12. Verfahren nach Anspruch 10, dadurch gekennzeichnet, daß  
ein Teil des Datenübertragungsverkehrs über die Schnittstelle  
(5) zum Telefon-Netz und ein weiterer Teil über eine Leitung

35 (1), die zum Übertragen des verschlüsselten Fernseh-Programms

GEÄNDERTES BLATT

mit dem Fernsehgerät (TV) verbunden ist, mit oder vor einem das verschlüsselte Fernseh-Programm wiedergebenden Nutzsignal hin- bzw. herübertragen wird, wobei die zu übertragende Information so unterteilt und übertragen wird, daß sie nur wechselweise und  
5 auch nur stufenweise in jeweiliger Kenntnis entschlüsselt werden kann.

GEÄNDERTES BLATT

## PCT

WELTORGANISATION FÜR GEISTIGES EIGENTUM  
Internationales Büro

**INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE  
INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)**

<p>(51) Internationale Patentklassifikation <sup>6</sup> :  <b>H04N 7/16</b></p>	<p><b>A1</b></p>	<p>(11) Internationale Veröffentlichungsnummer: <b>WO 99/08446</b></p> <p>(43) Internationales  Veröffentlichungsdatum: 18. Februar 1999 (18.02.99)</p>
<p>(21) Internationales Aktenzeichen: PCT/EP98/04424</p> <p>(22) Internationales Anmeldedatum: 16. Juli 1998 (16.07.98)</p> <p>(30) Prioritätsdaten:  197 34 071.7 6. August 1997 (06.08.97) DE</p> <p>(71) Anmelder (für alle Bestimmungsstaaten ausser  US): DEUTSCHE TELEKOM AG [DE/DE];  Friedrich-Ebert-Allee 140, D-53113 Bonn (DE).</p> <p>(72) Erfinder; und</p> <p>(75) Erfinder/Anmelder (nur für US): WILHELM, Siegfried  [DE/DE]; Spitzwegstrasse 4, D-81373 München (DE).  KOWALSKI, Bernd [DE/DE]; Am Bastenberg 4, D-57072  Siegen (DE).</p> <p>(74) Gemeinsamer Vertreter: DEUTSCHE TELEKOM AG; Tech-  nologiezentrum, Patentabteilung EK03, D-64307 Darmstadt  (DE).</p>		<p>(81) Bestimmungsstaaten: CA, CN, JP, KR, TR, US, europäisches  Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR,  IE, IT, LU, MC, NL, PT, SE).</p> <p><b>Veröffentlicht</b>  <i>Mit internationalem Recherchenbericht.</i></p>

(54) Title: TRANSCODER FOR DECODING ENCODED TV PROGRAMS

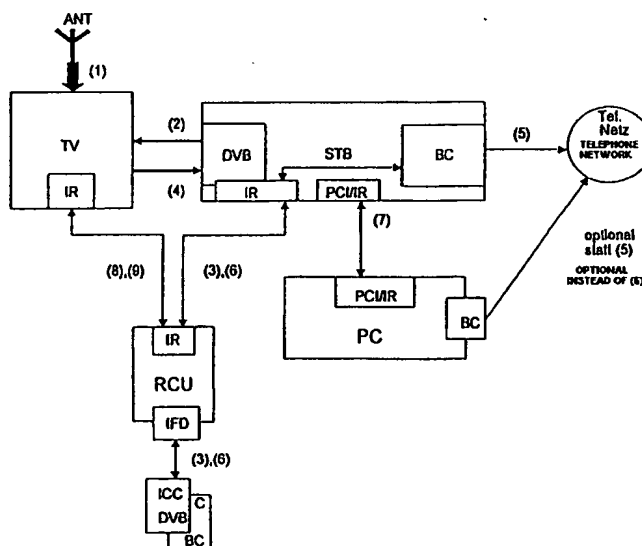
(54) **Bezeichnung:** DECODER-EINRICHTUNG FÜR DIE ENTSCHLÜSSELUNG VON VERSCHLÜSSELTEN FERNSEH-PROGRAMMEN

**(57) Abstract**

The invention pertains to a transcoder provided with a control unit and intended for decoding encoded TV programs. Said transcoder has an input for entering an encoded TV program, a decoding device for decoding an encoded TV program into a format which can be played on a television set, an output which can be connected to said television set and is designed to enter the encoded TV program into the television set for play, an interface for an identification or key component, to be used for validation of the decoding device, as well as an interface for a control unit in the transcoder. The transcoder according to the invention is characterized in that the interface for the identification or key component is located in said control unit.

### (57) Zusammenfassung

Decoder-Einrichtung mit einer Bedienungseinheit, für die Entschlüsselung von verschlüsselten Fernseh-Programmen, mit einem Eingang zum Einspeisen eines verschlüsselten Fernseh-Programmes, einer Entschlüsselungseinrichtung, die ein verschlüsseltes Fernseh-Programm in ein mittels eines Fernseh-Empfängers wiedergebares Format entschlüsselt, einem Ausgang, der mit einem Fernseh-Empfänger verbindbar ist, um das entschlüsselte Fernseh-Programm in den Fernseh-Empfänger zur Wiedergabe einzuspeisen, einer Schnittstelle für ein Identifikations- und/oder Schlüsselträgerbauteil zur Freigabe der Entschlüsselungseinrichtung, und einer Schnittstelle für eine Bedienungseinheit der Decoder-Einrichtung, wobei die Schnittstelle für das Identifikations- und/oder Schlüsselträgerbauteil in der Bedienungseinheit der Decoder-Einrichtung angeordnet ist.



# **LEDIGLICH ZUR INFORMATION**

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AL	Albanien	ES	Spanien	LS	Lesotho	SI	Slowenien
AM	Armenien	FI	Finnland	LT	Litauen	SK	Slowakei
AT	Österreich	FR	Frankreich	LU	Luxemburg	SN	Senegal
AU	Australien	GA	Gabun	LV	Lettland	SZ	Swasiland
AZ	Aserbaidschan	GB	Vereinigtes Königreich	MC	Monaco	TD	Tschad
BA	Bosnien-Herzegowina	GE	Georgien	MD	Republik Moldau	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagaskar	TJ	Tadschikistan
BE	Belgien	GN	Guinea	MK	Die ehemalige jugoslawische Republik Mazedonien	TM	Turkmenistan
BF	Burkina Faso	GR	Griechenland	ML	Mali	TR	Türkei
BG	Bulgarien	HU	Ungarn	MN	Mongolei	TT	Trinidad und Tobago
BJ	Benin	IE	Irland	MR	Mauretanien	UA	Ukraine
BR	Brasilien	IL	Israel	MW	Malawi	UG	Uganda
BY	Belarus	IS	Island	MX	Mexiko	US	Vereinigte Staaten von Amerika
CA	Kanada	IT	Italien	NE	Niger	UZ	Usbekistan
CF	Zentralafrikanische Republik	JP	Japan	NL	Niederlande	VN	Vietnam
CG	Kongo	KE	Kenia	NO	Norwegen	YU	Jugoslawien
CH	Schweiz	KG	Kirgisistan	NZ	Neuseeland	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Demokratische Volksrepublik Korea	PL	Polen		
CM	Kamerun	KR	Republik Korea	PT	Portugal		
CN	China	KZ	Kasachstan	RO	Rumänien		
CU	Kuba	LC	St. Lucia	RU	Russische Föderation		
CZ	Tschechische Republik	LI	Liechtenstein	SD	Sudan		
DE	Deutschland	LK	Sri Lanka	SE	Schweden		
DK	Dänemark	LR	Liberia	SG	Singapur		
EE	Estland						

-1-

Decoder-Einrichtung für die Entschlüsselung von verschlüsselten Fernseh-Programmen

- Die Erfindung betrifft eine Decoder-Einrichtung für die Entschlüsselung von verschlüsselten Fernseh-Programmen. Insbesondere betrifft die Erfindung eine Decoder-Einrichtung mit einer Bedienungseinheit, für die Entschlüsselung von verschlüsselten Fernseh-Programmen, mit einem Eingang zum Einspeisen eines verschlüsselten Fernseh-Programmes, einer Entschlüsselungseinrichtung, die ein verschlüsseltes Fernseh-Programm in ein mittels eines Fernseh-Empfängers wiedergegbares Format entschlüsselt, einem Ausgang, der mit einem Fernseh-Empfänger verbindbar ist, um das entschlüsselte Fernseh-Programm in den Fernseh-Empfänger zur Wiedergabe einzuspeisen, einer Schnittstelle für ein Identifikations- und/oder Schlüsselträgerbauteil zur Freigabe der Entschlüsselungseinrichtung, und einer Schnittstelle für eine Bedienungseinheit der Decoder-Einrichtung.
- Mit einer derartigen Decoder-Einrichtung ist der Empfang und die Entschlüsselung von sog. Pay-TV Programmen möglich, wobei derzeitige Decoder-Einrichtungen als sog. Set-Top-Boxen zu herkömmlichen Fernseh-Empfängern im Handel erhältlich sind.
- Die bisher üblichen, zum Beispiel monatlichen Abrechnungen, für die Bereitstellung des Programms bei Pay-TV weichen mehr und mehr einer individuellen ("pay-per-view") Abrechnungs-Praxis. Daher besteht die Notwendigkeit einer Identifizierung und Authentifizierung des Programm-Kunden vor dem Zugriff des Programm-Kunden auf das Programm. Außerdem werden bei sog. HOT-Programmen (Home Order Television) auch Bestellungen des Programm-Kunden gegen dessen Bankkonto oder seine Guthaben auf einer Chip-Karte verrechnet. Auch hierbei sind Identifizierung und Authentifizierung des Programm-Kunden sowie ggf. Sicherungs-Mechanismen gegen Mißbrauch erforderlich.

Zur Sicherung elektronischer Abrechnungsverfahren sowie zum Schutz vertraulicher Informationen (Bankverbindungsdaten, Konto-Stand etc.) werden Chipkarten eingesetzt, die Microprozessoren haben, die mit Verschlüsselungsalgorithmen ausgestattet sind. Ein derartiger Verschlüsselungsalgorithmus ist der sog. RSA-Algorithmus. Beim Pay-TV ist eine derartige Chipkarte Teil des sog. "Conditional Access System" (CAS), mit der geprüft wird, ob der Anfragende tatsächlich der autorisierte Programm-Kunde ist, und ggf. ob seine Bonität für die gewünschte Leistung ausreicht. Auch bei sog. "Electronic Commerce" repräsentiert diese Chipkarte die Identität des Kunden bzw. seine elektronische Geldbörse. Dabei kann auf der Chipkarte ein Guthaben vermerkt sein, das aufgefüllt werden kann. Zugriffe auf die Chipkarte durch Dritte (Programm-Provider, Handel oder dergl. Erfolgen in der Regel durch mehr oder weniger automatisierten telefonischen oder Internet-Kontakt mit der Set-Top-Box vor oder bei der Transaktion.

Ein wachsendes Problem in diesem Zusammenhang ist die steigende Anzahl von Anbietern von Programmen oder Leistungen, die ein Programm-Kunde über diese Medien beziehen kann. Damit wird auch der Geräte-Aufwand (Set-Top-Box, Fernseh-Gerät, Internet-Endgerät (PC oder Net-PC), Fernbedienungsgeräte für die Set-Top-Box und das Fernseh-Gerät, sowie die Anzahl der für die Inanspruchnahme der einzelnen Dienste oder Leistungen notwendigen Chip-Karten immer größer.

Der vorliegenden Erfindung liegt daher die Aufgabe zugrunde, diese unterschiedlichen Komponenten preiswerter zu gestalten, das heißt ihren Hardware-Aufwand zu verringern, und diese unterschiedlichen Komponenten in der Handhabung für den Programm-Kunden einfacher und fehlerunanfälliger zu gestalten. Außerdem soll die Erfindung dem in steigendem Maß relevanten Problem der Sicherheit im Zusammenhang mit der Leistungs-Inanspruchnahme durch unbefugte Dritte Rechnung tragen.



Erfindungsgemäß wird diese Aufgabe dadurch gelöst, daß die Schnittstelle für das Identifikations- und/oder Schlüsselträgerbauteil in der Bedienungseinheit der Decoder-Einrichtung angeordnet ist.

5

Durch diese Ausgestaltung können Schnittstellen eingespart werden. Außerdem ist der Programm-Kunde (Benutzer) auf bequemere Weise in der Lage, seine Transaktionen auszuführen, da die Bedienungseinheit der Decoder-Einrichtung ohnehin mit einem Tastenfeld ausgestattet ist. Weiterhin erhöht sich die Sicherheit, da der Programm-Kunde (auch in größerem Kreis von Dritten seine Eingaben (PIN, TAN, etc.) tätigen kann, ohne daß dies von Dritten beobachtet werden kann. Außerdem kann die Bedienungseinheit der Decoder-Einrichtung zusammen mit dem Identifikations- und/oder Schlüsselträgerbauteil (= Chipkarte) sicher verwahrt werden, während in der Regel aus Bequemlichkeit eine Chipkarte nicht aus der Decoder-Einrichtung (= Set-Top-Box) entnommen wird.

20 Gemäß einer bevorzugten Ausführungsform der erfindungsgemäßen Decoder-Einrichtung mit einer Bedienungseinheit ist die Bedienungseinheit auch zur Bedienung des Fernseh-Empfänger-Gerätes eingerichtet, der eine Schnittstelle zum Empfang von Steuerbefehlen von der Bedienungseinheit aufweist. Dies reduziert den Geräte-Aufwand weiter. Außerdem kann damit auch der Zugriff auf das Fernseh-Empfänger-Gerät insgesamt kontrolliert werden. Das heißt, daß auch die Benutzung des Fernsehers für nicht zahlungspflichtige Programme nur bei Freigabe durch den autorisierten Benutzer möglich ist.

25 Dies kann dadurch erreicht werden, daß die Funktion der Bedienungseinheit als Ganzes von der Eingabe der Kennung (PIN) des autorisierten Benutzer abhängt.

Insbesondere zur Abwicklung der Abbuchungen und zur Identifizierung und des Programm-Kunden durch der Programm-Anbieter dient bei der erfindungsgemäßen Decoder-Einrichtung eine Schnittstelle zu einem Telekommunikationsnetz. Dies kann ein MODEM sein. Oder für digitale Telekommunikationsnetze eine entsprechende Ankopplungseinrichtung sein.

35

Insbesondere zur Erhöhung der Sicherheit in dem System dient eine Schnittstelle zu einem Identifikations- und/oder Schlüsselträgerbauteil, durch das der Programm-Kunde über die oben beschriebene Schnittstelle zu einem Telekommunikationsnetz zu einem Dienste-Anbieter oder Waren-Versender Kontakt aufnehmen kann. Auch hier erfolgt die Herstellung einer Verbindung über das Telekommunikationsnetz mit einem bestimmten Teilnehmer (Dienste-Anbieter oder Waren-Versender) abhängig von einer Authorisierung durch das Identifikations- und/oder Schlüsselträgerbauteil erfolgt. Damit ist der Programm-Anbieter unabhängig von dem Dienste-Anbieter oder Waren-Versender in der Abrechnung mit dem Programm-Kunden. Dies kann Vorteile hinsichtlich der Datensicherheit und der Flexibilität mit sich bringen.

Alternativ dazu ist es jedoch auch möglich, daß der Programm-Anbieter mit dem Dienste-Anbieter eine geeignete Kooperation hat, so daß eine gemeinsame Abrechnung bzw. Kunden-Verwaltung und damit auch Kunden-Identifizierung und Kunden-Authorisierung erfolgen kann. In diesem Fall sind keine getrennten Chip-Karten erforderlich.

Unabhängig davon ist es vorteilhaft, wenn auch die Schnittstelle zu dem Identifikations- und/oder Schlüsselträgerbauteil für die Authorisierung der Verbindung über das Telekommunikationsnetz in der Bedienungseinheit angeordnet ist.

Wie bereits erwähnt können das Identifikations- und/oder Schlüsselträgerbauteil für die Authorisierung der Verbindung über das Telekommunikationsnetz und das Identifikations- und/oder Schlüsselträgerbauteil zur Freigabe des Entschlüsselungseinrichtung entweder durch zwei getrennte oder durch eine gemeinsame Chip-Karte realisiert sein.

In einer weiteren Ausgestaltung weist die Decoder-Einrichtung eine Schnittstelle auf, über die die Decoder-Einrichtung mit einem Rechner verbindbar ist, der zur Steuerung der Decoder-Einrichtung und/oder zur Herstellung einer Verbindung mit einem anderen Teilnehmer über das Telekommuni-

kationsnetz eingerichtet ist. Damit ist es möglich, die gesamten Funktionalität eines Rechners (PC oder Internet-PC), also die Speicherung und Verarbeitung von Daten und Informationen, sowie die komfortablere Gestaltung von Dialogen des Programm-Kunden mit zum Beispiel dem Programm-Anbieter oder dem Dienste-Anbieter für den Programm-Kunden verfügbar zu machen.

In einer besonders bevorzugten Ausführungsform der Erfindung ist die Bedienungseinheit durch den Rechner gebildet ist, der eine Schnittstelle aufweist, um die Decoder-Einrichtung zu steuern, und eine Schnittstelle für das Identifikations- und/oder Schlüsselträgerbauteil für die Autorisierung der Verbindung über das Telekommunikationsnetz bzw. das Identifikations- und/oder Schlüsselträgerbauteil zur Freigabe des Entschlüsselungseinrichtung aufweist. Damit wird die Bereitstellung einer bzw. zwei separaten Bedienungseinheiten überflüssig. Es versteht sich, daß auch bei dieser Ausführungsform die beiden Chip-Karten für den Verkehr mit dem Programm-Anbieter und dem Dienste-Anbieter auch als eine gemeinsame Chip-Karte realisiert sein können.

Im übrigen kann die Verbindung zwischen dem Rechner und dem Fernseh-Gerät bzw. dem Rechner und der Decoder-Einrichtung sowohl drahtlos (zum Beispiel als Infrarot- oder als Ultraschallverbindung), als auch drahtgebunden sein kann. Außerdem kann der Rechner wegen seiner speziellen Anforderungen (relativ geringer Speicherbedarf, geringe Anforderungen an den Tastaturkomfort wegen der üblicherweise nur kurzen Eingaben etc.) auch als sog. Palmtop-Rechner ausgestaltet sein, der mit entsprechenden Schnittstellen (Infrarot-Schnittstelle zu der Decodier-Einrichtung so einer oder mehreren Schnittstellen für die Chip-Karte(n). Damit hat der Benutzer eine sehr kompakte und komfortable Steuerungs- und Bedienmöglichkeit seiner Geräte, aber auch die einfache Möglichkeit, mit dem Programm-Anbieter und/oder dem Dienste/Waren-Anbieter auf komfortable Weise zu kommunizieren. Schließlich verringert sich auch der Verkabelungsaufwand

zwischen den einzelnen Komponenten auf der Benutzerseite erheblich, was ebenfalls den Komfort erhöht.

Gemäß einer besonders bevorzugten Ausführungsform der Erfindung ist die Decoder-Einrichtung in das Fernsehgerät integriert. Damit wird dem Benutzer ein geschlossenes und gegen Mißbrauch besonders geschütztes Gerät zur Verfügung gestellt, bei dem alle Funktionen (herkömmliches Fernsehen, Pay-TV, Kommunikation mit einem Dienste/Waren-Anbieter über das Telekommunikationsnetz, Speicherung und/oder Nachbearbeitung der empfangenen Daten in dem Rechner etc.) in einer gegen Mißbrauch geschützten Weise ausführbar sind.

Die Erfindung betrifft auch eine Chip-Karte für eine vorstehend beschriebene Decoder-Einrichtung mit einer Bedienungseinheit, mit einer Rechneinheit, einem ersten Speicherbereich, in dem zumindest Teile von Betriebssystem-Funktionen abgelegt sind, mit denen die Kommunikation zwischen der Rechneinheit der Chip-Karte und den Peripherie-Geräten der Chip-Karte, sowie die Kommunikation mit einem externen Host-Rechner gesteuert wird, und mit denen geschützte, ungeschützte, und/oder Schreib/Lese-Speicher-Bereiche der Chip-Karte verwaltet werden, und einem zweiten Speicherbereich, der in geschützte und ungeschützte Bereiche unterteilt ist, wobei der Zugriff auf geschützte Bereiche in Abhängigkeit von einem Ergebnis einer Überprüfung der Zulässigkeit des Zugriffs erfolgt, wobei in dem geschützten Bereich des zweiten Speicherbereiches ein Generalschlüssel abgelegt ist, unter dessen Kontrolle die Eintragung wenigstens eines weiteren einfachen Schlüssels sowie eines zu diesem weiteren einfachen Schlüssel gehörendes Protokoll-Programm durch den externen Host-Rechner erfolgt.

Mit dieser Chip-Karte kann die vorstehend beschriebene Decoder-Einrichtung besonders sicher betrieben und auch einfach um den Zugriff auf mehrere weitere Dienste-Anbieter erweitert werden.

Vorzugsweise ist in dem zweiten Speicherbereich eine Schlüssel-Verwaltung abgelegt, von der aus der Zugriff auf ein Protokoll-Programm eines einfachen Schlüssels erfolgt.

- 5 Zur Ergänzung zusätzlicher Schlüssel bzw. Zugriffsmöglichkeiten auf weitere Anbieter dient dabei folgendes erfindungsgemäße Verfahren:
- Herstellen einer Telekommunikationsverbindung zwischen dem Host-Rechner und der Decoder-Einrichtung mit der Bedie-
  - 10 nungseinheit oder dem die Bedienungseinheit enthaltenden Rechner durch den Host-Rechner,
  - Überprüfen des Generalschlüssels in der Chip-Karte durch den Host-Rechner,
  - Übermitteln eines einfachen Schlüssels sowie eines zu
  - 15 diesem Schlüssel gehörenden Protokoll-Programmes an die Chip-Karte in verschlüsselter Form, falls die Überprüfung positiv ausfällt,
  - Eintragen des einfachen Schlüssels sowie des zu diesem Schlüssel gehörenden Protokoll-Programmes in den geschütz-
  - 20 ten Speicherbereich der Chip-Karte,
  - Sperren des geschützten Speicherbereiches der Chip-Karte.

Dabei kann vor dem Eintragen des einfachen Schlüssels sowie des zu diesem Schlüssel gehörenden Protokoll-Programmes in

25 den geschützten Speicherbereich der Chip-Karte der Schlüssel und das Protokoll-Programm durch die Rechneinheit der Chipkarte entschlüsselt werden.

Fig. 1 zeigt eine Anordnung gemäß dem Stand der Technik in

30 einem schematischen Blockdiagramm.

Fig. 2 - 4 zeigen unterschiedliche Ausführungsformen der vorliegenden Erfindung, jeweils in einem schematischen Blockdiagramm.

35

Fig. 1 zeigt eine derzeit übliche Endgeräteumgebung für kombinierte Pay TV- und Electronic-Commerce Anwendungen.

Über die Leitung (1) wird das breitbandige digital verschlüsselte Pay TV Nutzsignal durch das Fernseh-Gerät empfangen und über den Ausgang (4) an den Eingang (IN) in die Set-Top-Box (STB) übergeben. Dort wird das Signal von einem  
5 speziellen Chip mit einem hierfür vorgesehenen Algorithmus - der DVB-Algorithmus sei hier stellvertretend für alle genannt - entschlüsselt und an das Fernseh-Gerät zurückgegeben. Die Einstellung der Schlüssel erfolgt mittels einer Chipkarte (ICC DVB) über die Schnittstelle (3). Die Chip-  
10 karte enthält den Schlüsselverteilalgorithmus des Conditional Access Systems (z. B. RSA) und den geheimen Schlüssel des Kunden. Nur ein Kunde mit gültiger Chipkarte (ICC DVR) kann Pay TV Sendungen entschlüsseln. Die Chipkarte (ICC DVR) ist über die Chipkarten-Schnittstelle "IFD" an die  
15 Set-Top-Box (STB) angeschlossen.

Erweiterungen der Set-Top-Box (STB) sehen vor, daß ein Rückkanal über das Telefonnetz bzw. Internet über die Schnittstelle (5) mit den Servern verschiedener Dienstleis-  
20 stungsanbieter verbunden werden kann, um z.B. Dienstleistungen oder Artikel zu bestellen, die als Angebot in der Werbung der Pay TV Kanäle enthalten sind. Zur Sicherung von Bestellung und Bezahlung kann hier eine zweite Chipkarte (ICC BC) über eine weitere Schnittstelle (IFD) eingesteckt  
25 werden, so daß die Verbindung (6) zwischen der zweiten Chipkarte (ICC BC) und der weiteren Schnittstelle (IFD) hergestellt ist.

Weitere Anschlußmöglichkeiten der Set-Top-Box (STB) sehen  
30 die Verwendung einer IR-Fernbedienung (9) und eines Rechners PC über eine im PC-Umfeld übliche Schnittstelle (7), hier vereinfachend "PCI" genannt (z.B. V24/RS232C oder parallele Schnittstelle), vor. Mit dem Rechner PC lassen sich z.B. Rückkanalgeschäfte komfortabel gestalten oder Informa-  
35 tionen aus den Pay TV Kanälen nachverarbeiten.

Zum Anschluß zweier Chipkarten an die Set-Top-Box (STB) gibt es verschiedene Lösungen. Entweder werden die Chipkartenterminals (IFD) fest in die Set-Top-Box (STB) einge-

baut oder sie werden steckbar als PCMCIA-Module ausgeführt. Mit Hilfe der PCMCIA Module entsteht die Möglichkeit, verschiedene Pay TV Zugangsverfahren (CAS) ohne Eingriffe in die Set-Top-Box (STB) gegeneinander auszuwechseln.

5

Nachteile der herkömmlichen Endgeräte-Konfiguration sind die geringe Bedienungsfreundlichkeit, die umständliche Verkabelung der Set-Top-Box (STB) und deren aufwendige Schnittstellengestaltung.

10

Die Fig. 2, 3 und 4 illustrieren Ausführungsformen der Erfindung.

15

Bereits in einer ersten Integrationsstufe nach Fig. 2 werden die Fernbedienungen von Set-Top-Box (STB) und Fernsehgerät (TV Set) in einem Gerät, der Bedienungseinheit (RCU) zusammengefaßt. Die neue Bedienungseinheit (RCU) erhält eine Chipkartenschnittstelle, die sowohl die Chipkarte (ICC DVB) des Pay TV Systems als auch die Chipkarte (ICC BC) des Rückkanals ansteuern kann. Der Schlüsselaustausch des Conditional Access Systems CAS des PAY TV geschieht zwar vom Ablauf her genauso wie in der herkömmlichen Konfiguration.

20

25

In Fig. 2 ist die Chip-Karte (ICC) DVB jedoch über die Bedienungseinheit (RCU) durch eine IR-Schnittstelle mit dem Pay TV Entschlüsselungschip (z. B. DVB) in der Set-Top-Box (STB) verbunden. Das Gleiche gilt für die Chip-Karte (ICC) BC, welche die Sicherung des Rückkanals nunmehr ebenfalls über die Bedienungseinheit (RCU) und deren IR-Schnittstelle vornimmt.

30

35

Damit entfällt das Einstecken der Chipkarten in die Set-Top-Box (STB) und somit auch alle Chipkartenschnittstellen an der Set-Top-Box (STB). Der Kunde steckt seine Karten direkt in die Fernbedienung RCU. Falls Pay-TV-Anbieter und Rückkanal-Dienstleister entsprechende vertragliche Vereinbarungen treffen, können die Funktionen beider Chipkarten ICC DVB und ICC BC sogar auf einer einzigen Chip-Karte (ICC) zusammengefaßt werden.

Der Rechner PC wird in Fig. 2ff entweder weiterhin über eine herkömmliche Schnittstelle (PCI) mit der Set-Top-Box (STB) verbunden oder nutzt hierzu ebenfalls die IR-Schnittstelle (Infra-Rot-Schnittstelle) der Set-Top-Box (STB).

Die Rückkanalanbindung an das Telekommunikationsnetz erfolgt entweder über die Set-Top-Box (STB) oder über den Rechner (PC). Grundsätzlich sind beide Varianten möglich.

Fig. 3 zeigt die Kombination von Fernbedienung (RCU) und dem Rechner (PC) in einer weiteren Integrationsstufe. Hierbei lassen sich die Vorteile des Rechners PC und der Fernbedienung (RCU) gleichzeitig nutzen. Diese Lösung wird insbesondere interessant, wenn es sich bei dem kombinierten Gerät RCU/PC um ein "Netzwerk-PC"-ähnliches Gerät handelt, welches kompakt und ohne aufwendige Peripherie und Verkabelung z.B. vom Wohnzimmertisch aus bedient werden kann.

In Fig. 4 ist die Vereinigung von Fernseh-Gerät (TV Set) und Set-Top-Box (STB) in nur einem Endgerät als eine weitere Integrationsstufe dargestellt.

Die in den Fig. 2 bis 4 dargestellten neuen Endgeräte-Konfigurationen zeigen, wie sich die Bedienung und die Verkabelung der Endgeräte nennenswert vereinfachen läßt ohne die Funktionalität zu beeinträchtigen.

Erfindungsgemäß werden also anstelle einer oder mehrerer Chipkartenschnittstellen an der Set-Top-Box (STB) nunmehr die betreffenden Chipkarten über eine Fernbedienung RCU und deren Infrarot-Schnittstellen mit dem in der Set-Top-Box (STB) verbleibenden Pay TV Entschlüsselungschip verbunden. Damit können aufwendige und anfällige Schnittstellen an der Set-Top-Box (STB) entfallen.

Außerdem können die Funktionen der Pay TV Chipkarte und der Rückkanal Chipkarte unter Zuhilfenahme einer speziellen



Fernbedienung RCU auf nur einer Karte bedienungsfreundlich kombiniert werden.

Schließlich ist durch die Kombination von Fernbedienung und  
5 PC in nur einem Gerät RCU/PC eine Verlagerung der Rückkanalanbindung aus der Set-Top-Box (STB) heraus ermöglicht. Damit ist eine optimale Nutzung des Internet PC (= PC, der über beliebige Online-Netze mit Servern von beliebigen Diensteanbietern verbunden ist), in Verbindung mit Pay TV  
10 Diensten einschließlich ihrer Rückkanaloptionen ermöglicht.

Ein weiterer Gesichtspunkt der Erfindung ist die Ausgestaltung der Chip-Karte, damit diese auch in der Lage ist, mit hohem Sicherheits-Niveau sowohl die Programm-Entschlüsselung des Programms des Pay-TV-Anbieters, als auch die  
15 Transaktion (Bestellung und Kaufpreis-Entrichtung) bei dem Waren/Dienstleistungs-Anbieter abzuwickeln.

Insbesondere, wenn im Laufe der Zeit weitere Waren/Dienstleistungs-Anbieter dazukommen, hätte dies zur Folge, daß der Programm-Kunde jeweils eine neue Chip-Karte benötigt, die die Schlüssel und Protokolle der bisherigen Anbieter (sowohl Pay-TV-Anbieter, als auch Waren/Dienstleistungs-Anbieter) enthält, als auch den Schlüssel und das Protokoll  
20 des neu dazugekommenen.

Hierfür bietet die Erfindung ebenfalls eine Lösung:  
Da der Waren/Dienstleistungs-Anbieter ohnehin in der Regel durch den gleichen Host-Rechner mit dem Benutzer in Verbindung tritt wie der Pay-TV-Anbieter, kann dieser Host auch  
30 über einen Generalschlüssel auf die gesperrten Bereiche der Chip-Karte des Kunden zugreifen, um dort einen weiteren Schlüssel und das zugehörige Protokoll für zukünftige Transaktionen (Entschlüsselungs- oder Zahlungsvorgänge) abzulegen.  
35

Außerdem ist in einem weiteren (ggf. ebenfalls gesperrten) Bereich eine Vektorentabelle oder eine Abfrage-Routine zu führen, in der nacheinander die neu dazukommenden Schlüssel

verwaltet werden. Beim Zugriff auf die Chipkarte wird zunächst anhand der Vektorentabelle oder der Abfrage-Routine geprüft, ob ein passender Schlüssel vorhanden ist, bzw. ob der durch den Benutzer eingegebene Schlüssel mit einem der  
5 auf der Chip-Karte abgelegten Schlüssel zusammenpaßt. Erst wenn das Ergebnis dieser Abfrage positiv ist, wird das zu dem jeweiligen Schlüssel gehörige Programm zur Transaktion bzw. Entschlüsselung (ggf. entschlüsselt und dann) ausgeführt.

10

Vorzugsweise wird der Schlüssel und das zugehörige Protokoll(-Programm) in ebenfalls verschlüsselter Form von dem Host-Rechner an die Set-Top-Box (STB) übertragen, und von dort über die Schnittstelle an die Bedienungseinheit (RCU)  
15 weitergegeben. Falls die Bedienungseinheit (RCU) in den Rechner (PC/RCU) integriert ist, kann der Host-Rechner Rechner direkt über das Telekommunikationsnetz mit dem Rechner (PC/RCU) in Verbindung treten, um die Informationen für die bzw. in die Chip-Karte (ICC) zu übertragen.

20

Je nach konkreter Ausgestaltung kann das Protokoll(-Programm) in der Chip-Karte nur in verschlüsselter Form abgelegt sein, und jeweils zur Laufzeit vor der Ausführung entschlüsselt werden. Alternativ dazu kann das Protokoll(-Programm)  
25 jedoch auch beim Ablegen in dem (geschützten) Speicherbereich der Chipkarte in eine lauffähige Form gebracht werden.

Damit enthält der Speicher der Chip-Karte (neben anderem)  
30 folgende Programme bzw. Daten:

Einen Betriebssystem-Kern, mit dem die Kommunikation zwischen dem Prozessor der Chip-Karte und den Peripherie-Geräten auf der Chip-Karte, sowie die Kommunikation mit dem  
35 Host-Rechner gesteuert wird, der die Speicherbereiche der Chip-Karte (geschützte und ungeschützte Bereiche, Schreib/Lese-Bereiche, Flash-EEPROM etc.) verwaltet usw.

- Schlüssel (ein Haupt- oder General-Schlüssel, sowie ein oder mehrere Anwendungs-Schlüssel), wobei der Haupt-Schlüssel dazu dient, (weitere) Anwendungs-Schlüssel und die zugehörigen Anwendungs- oder Protokoll-Programme in den Speicher-Bereich zu transferrieren. Die Anwendungs-Schlüssel dienen dazu sicherzustellen, daß die Ausführung der Protokoll-Programme (und damit der Abwicklung von Bestellungen oder die Entschlüsselung von Pay-TV-Programmen) nur bei Vorliegen der richtigen Eingabe durch den Benutzer erfolgt.
- 10 Verschlüsselte Anwender-Programme oder Protokoll-Programme, mit denen die Abwicklung von Bestellungen oder die Entschlüsselung von Pay-TV-Programmen gesteuert wird.
- 15 Zur weiteren Erhöhung der Sicherheit ist es vorgesehen, die Identifizierung und Authentifizierung zwischen der Bedienungseinheit (RCU) und/oder der Set-Top-Box (STB) bzw. Fernseh-Gerät (TV Set) einerseits und dem Host-Rechner andererseits auf unterschiedlichen Wegen bzw. Kanälen durchzuführen. Mit anderen Worten werden ein Teil des Protokollverkehrs über die Schnittstelle (5) zum Telefon-Netz und ein weiterer Teil über die Leitung (1) mit oder vor dem breitbandigen digital verschlüsselten Pay TV Nutzsignal übertragen. Dabei kann auch die Freischaltung/Sperrung von
- 20 Diensten auf diesen Wegen erfolgen. Da für einen Mißbrauch dann beide Kanäle synchron abzuhören und zu entschlüsseln wären, ist so die Sicherheit erheblich höher. Insbesondere ist es möglich, die Informationen mit der Freischaltung/Sperrung oder neue Schlüssel etc. auf die beiden Kanäle so
- 25 zu verteilen, daß sie nur wechselweise und auch nur stufenweise in jeweiliger Kenntnis entschlüsselt werden können.
- 30

## Ansprüche

1. Decoder-Einrichtung mit einer Bedienungseinheit (RCU),  
für die Entschlüsselung von verschlüsselten Fernseh-  
5 Programmen, mit
- einem Eingang (4) zum Einspeisen eines verschlüsselten  
Fernseh-Programmes,
  - einer Entschlüsselungseinrichtung (DVB), die ein ver-  
schlüsseltes Fernseh-Programm in ein mittels eines Fernseh-  
10 Empfängers (TV Set) wiedergebares Format entschlüsselt,
  - einem Ausgang (2), der mit einem Fernseh-Empfänger (TV  
Set) verbindbar ist, um das entschlüsselte Fernseh-Programm  
in den Fernseh-Empfänger (TV Set) zur Wiedergabe einzuspei-  
sen,
  - 15 - einer Schnittstelle (IFD 3,6) für ein Identifikations-  
und/oder Schlüsselträgerbauteil (ICC DVB) zur Freigabe des  
Entschlüsselungseinrichtung (DVB), und
  - einer Schnittstelle (IR 3,6) für eine Bedienungseinheit  
(RCU) der Decoder-Einrichtung (DVB),
  - 20 dadurch gekennzeichnet, daß
  - die Schnittstelle (IFD 3,6) für das Identifikations-  
und/oder Schlüsselträgerbauteil (ICC DVB) in der Bedie-  
nungseinheit (RCU) der Decoder-Einrichtung (STB) angeordnet  
ist.
  - 25
2. Decoder-Einrichtung mit einer Bedienungseinheit (RCU)  
nach Anspruch 1, dadurch gekennzeichnet, daß
- die Bedienungseinheit (RCU) auch zur Bedienung des Fern-  
seh-Empfängers (TV Set) eingerichtet ist, der eine Schnitt-  
30 stelle (IR (,9) zum Empfang von Steuerbefehlen aufweist.
3. Decoder-Einrichtung mit einer Bedienungseinheit (RCU)  
nach Anspruch 1, gekennzeichnet durch
- eine Schnittstelle (BC 5) zu einem Telekommunikations-  
35 netz.

-15-

4. Decoder-Einrichtung mit einer Bedienungseinheit (RCU) nach Anspruch 3, gekennzeichnet durch
- eine Schnittstelle (IFD 3,6) zu einem Identifikations- und/oder Schlüsselträgerbauteil (ICC BC), wobei die Herstellung einer Verbindung über das Telekommunikationsnetz mit einem bestimmten Teilnehmer abhängig von einer Authorisierung durch das Identifikations- und/oder Schlüsselträgerbauteil (ICC BC) erfolgt.
5. Decoder-Einrichtung mit einer Bedienungseinheit (RCU) nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß
- die Schnittstelle zu dem Identifikations- und/oder Schlüsselträgerbauteil für die Authorisierung der Verbindung über das Telekommunikationsnetz in der Bedienungseinheit (RCU) angeordnet ist.
6. Decoder-Einrichtung mit einer Bedienungseinheit (RCU) nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß
- das Identifikations- und/oder Schlüsselträgerbauteil für die Authorisierung der Verbindung über das Telekommunikationsnetz und das Identifikations- und/oder Schlüsselträgerbauteil zur Freigabe des Entschlüsselungseinrichtung entweder durch zwei getrennte oder durch eine gemeinsame Chip-Karte realisiert sind.
7. Decoder-Einrichtung mit einer Bedienungseinheit (RCU) nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß
- die Decoder-Einrichtung eine Schnittstelle (DVB) aufweist über die die Decoder-Einrichtung mit einem Rechner (PC) verbindbar ist, der zur Steuerung der Decoder-Einrichtung und/oder zur Herstellung einer Verbindung mit einem anderen Teilnehmer über das Telekommunikationsnetz eingerichtet ist.

8. Decoder-Einrichtung mit einer Bedienungseinheit (RCU) nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß
- die Bedienungseinheit (RCU) durch den Rechner (PC) gebildet ist, der
  - eine Schnittstelle (IR 3,7) aufweist, um die Decoder-Einrichtung zu steuern, und
  - eine Schnittstelle (IFD 3,6) für das Identifikations- und/oder Schlüsselträgerbauteil (ICC BC) für die Autorisierung der Verbindung über das Telekommunikationsnetz bzw. das Identifikations- und/oder Schlüsselträgerbauteil (ICC DVB) zur Freigabe der Entschlüsselungseinrichtung (DVB) aufweist.
- 15 9. Decoder-Einrichtung mit einer Bedienungseinheit (RCU) nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß
- die Decoder-Einrichtung in das Fernsehgerät integriert ist.
- 20 10. Chip-Karte für eine Decoder-Einrichtung mit einer Bedienungseinheit (RCU) nach einem der vorhergehenden Ansprüche, mit
- einer Rechneinheit,
  - einem ersten Speicherbereich, in dem zumindest Teile von Betriebssystem-Funktionen abgelegt sind, mit denen die Kommunikation zwischen der Rechneinheit der Chip-Karte und den Peripherie-Geräten der Chip-Karte, sowie die Kommunikation mit einem externen Host-Rechner gesteuert wird, und
  - mit denen geschützte, ungeschützte, und/oder Schreib/Lese-Speicher-Bereiche der Chip-Karte verwaltet werden, und
  - einem zweiten Speicherbereich, der in geschützte und ungeschützte Bereiche unterteilt ist, wobei der Zugriff auf geschützte Bereiche in Abhängigkeit von einem Ergebnis einer Überprüfung der Zulässigkeit des Zugriffs erfolgt, dadurch gekennzeichnet, daß
  - in dem geschützten Bereich des zweiten Speicherbereiches ein Generalschlüssel abgelegt ist, unter dessen Kontrolle die Eintragung wenigstens eines weiteren einfachen Schlüs-

sels sowie eines zu diesem weiteren einfachen Schlüssel gehörendes Protokoll-Programm durch den externen Host-Rechner erfolgt.

11. Chip-Karte nach Anspruch 10, dadurch gekennzeichnet,  
5 daß

- in dem zweiten Speicherbereich eine Schlüssel-Verwaltung abgelegt ist, von der aus der Zugriff auf ein Protokoll-Programm eines einfachen Schlüssels erfolgt.

10 12. Verfahren zur Kommunikation eines Host-Rechners eines Pay-TV-Anbieters mit einer Decoder-Einrichtung mit einer Bedienungseinheit (RCU) nach einem der Ansprüche 1 - 9, und einer Chip-Karte nach einem der Ansprüche 10, 12 gekennzeichnet durch folgende Schritte:

15 - Herstellen einer Telekommunikationsverbindung zwischen dem Host-Rechner und der Decoder-Einrichtung mit der Bedienungseinheit oder dem die Bedienungseinheit enthaltenden Rechner durch den Host-Rechner,

- Überprüfen des Generalschlüssels in der Chip-Karte durch  
20 den Host-Rechner,

- Übermitteln eines einfachen Schlüssels sowie eines zu diesem Schlüssel gehörenden Protokoll-Programmes an die Chip-Karte in verschlüsselter Form, falls die Überprüfung positiv ausfällt,

25 - Eintragen des einfachen Schlüssels sowie des zu diesem Schlüssel gehörenden Protokoll-Programmes in den geschützten Speicherbereich der Chip-Karte,

- Sperren des geschützten Speicherbereiches der Chip-Karte.

30 13. Verfahren nach Anspruch 12, dadurch gekennzeichnet, daß

- vor dem Eintragen des einfachen Schlüssels sowie des zu diesem Schlüssel gehörenden Protokoll-Programmes in den geschützten Speicherbereich der Chip-Karte der Schlüssel und

35 das Protokoll-Programm vorzugsweise durch die Rechneinheit der Chipkarte entschlüsselt werden.

14. Verfahren nach Anspruch 12, dadurch gekennzeichnet, daß ein Teil des Datenübertragungsverkehrs über die

-18-

Schnittstelle (5) zum Telefon-Netz und ein weiterer Teil über die Leitung (1) mit oder vor dem breitbandigen digital verschlüsselten Pay TV Nutzsignal übertragen hin- bzw. herübertragen wird, wobei auf die zu übertragende Information  
5 auf die beiden Kanäle so verteilt ist, daß sie nur wechselseitig und auch nur stufenweise in jeweiliger Kenntnis entschlüsselt werden kann.



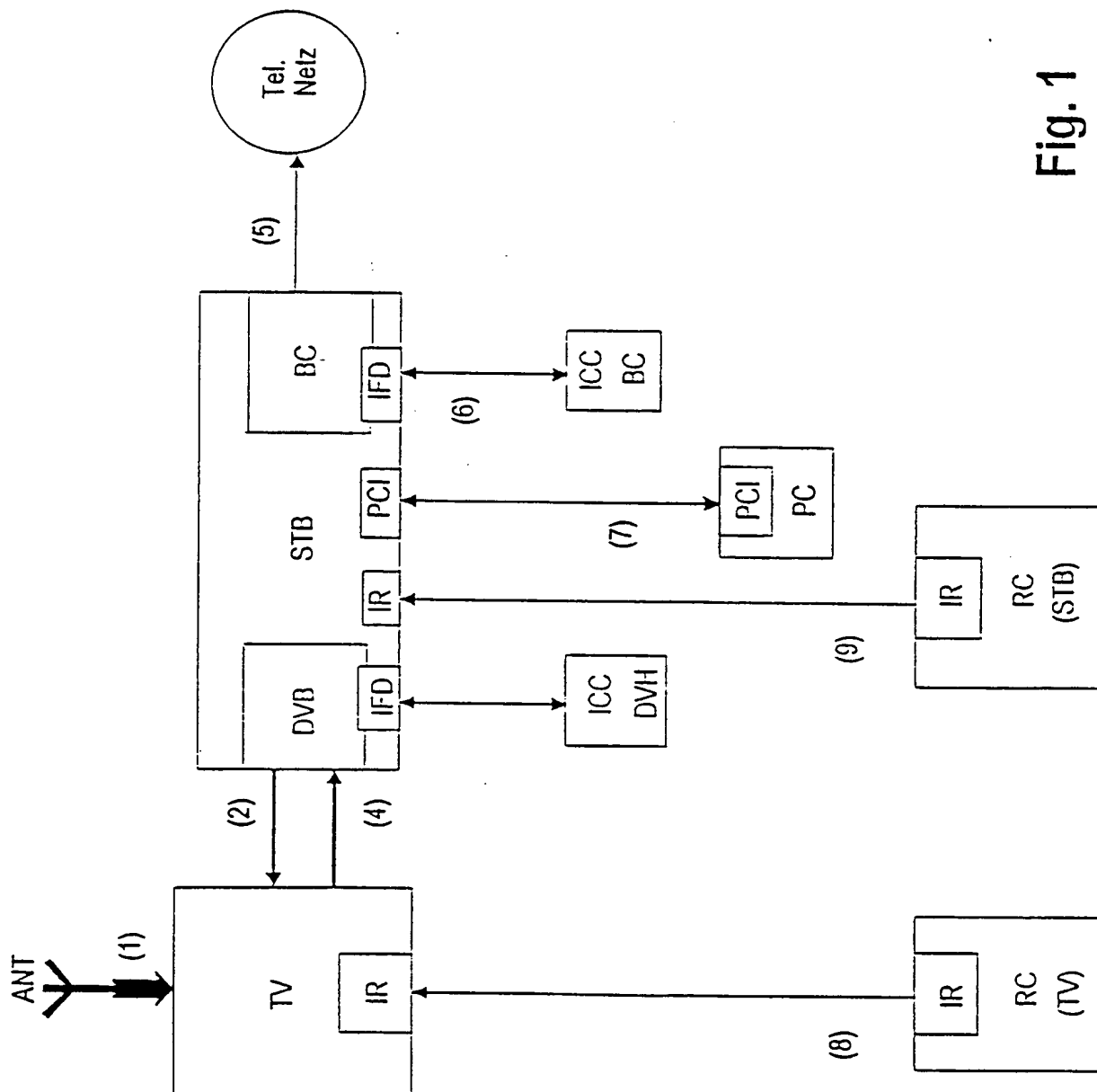


Fig. 1

**THIS PAGE BLANK (USPTO)**

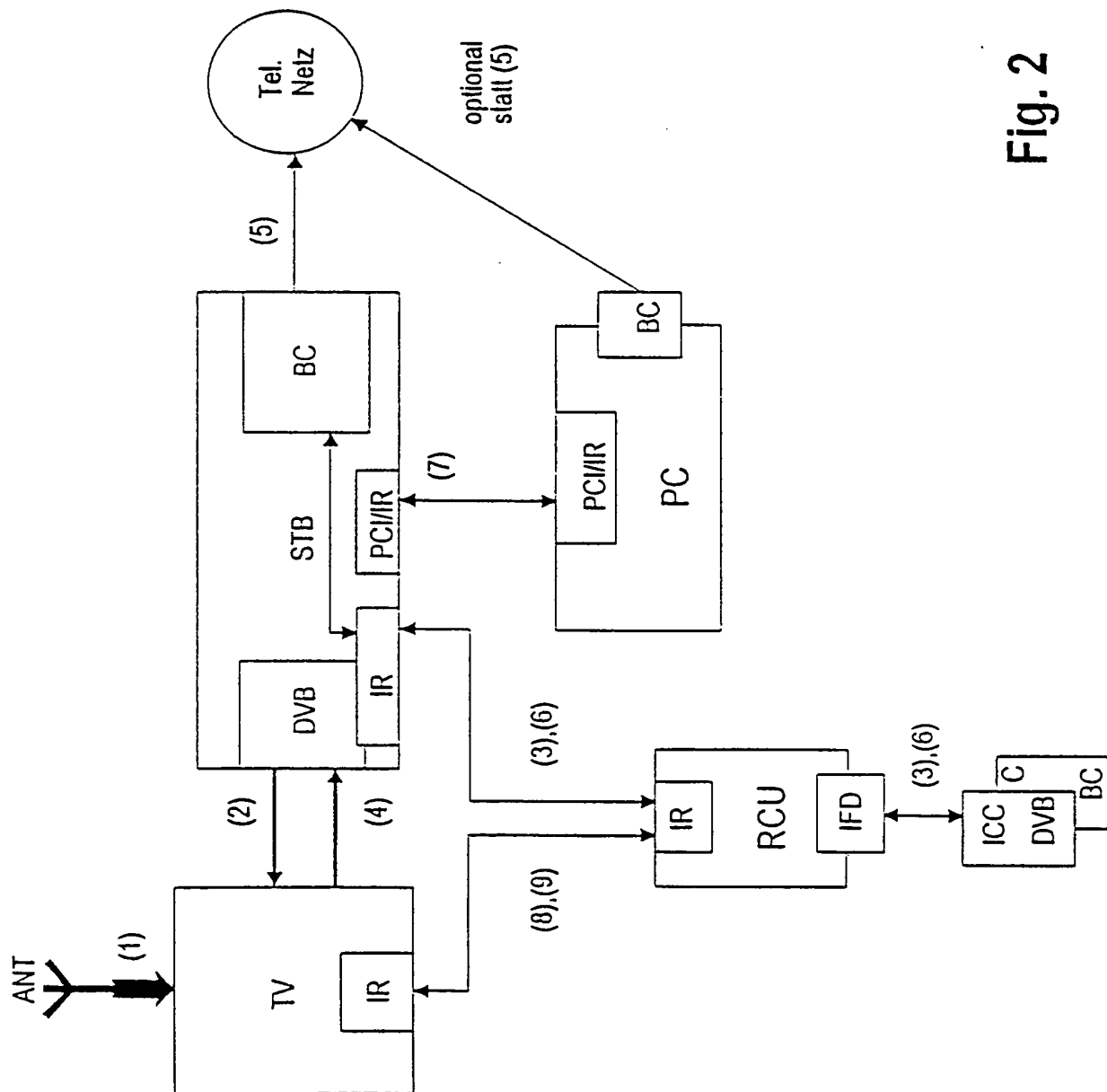


Fig. 2

**THIS PAGE BLANK (USPTO)**

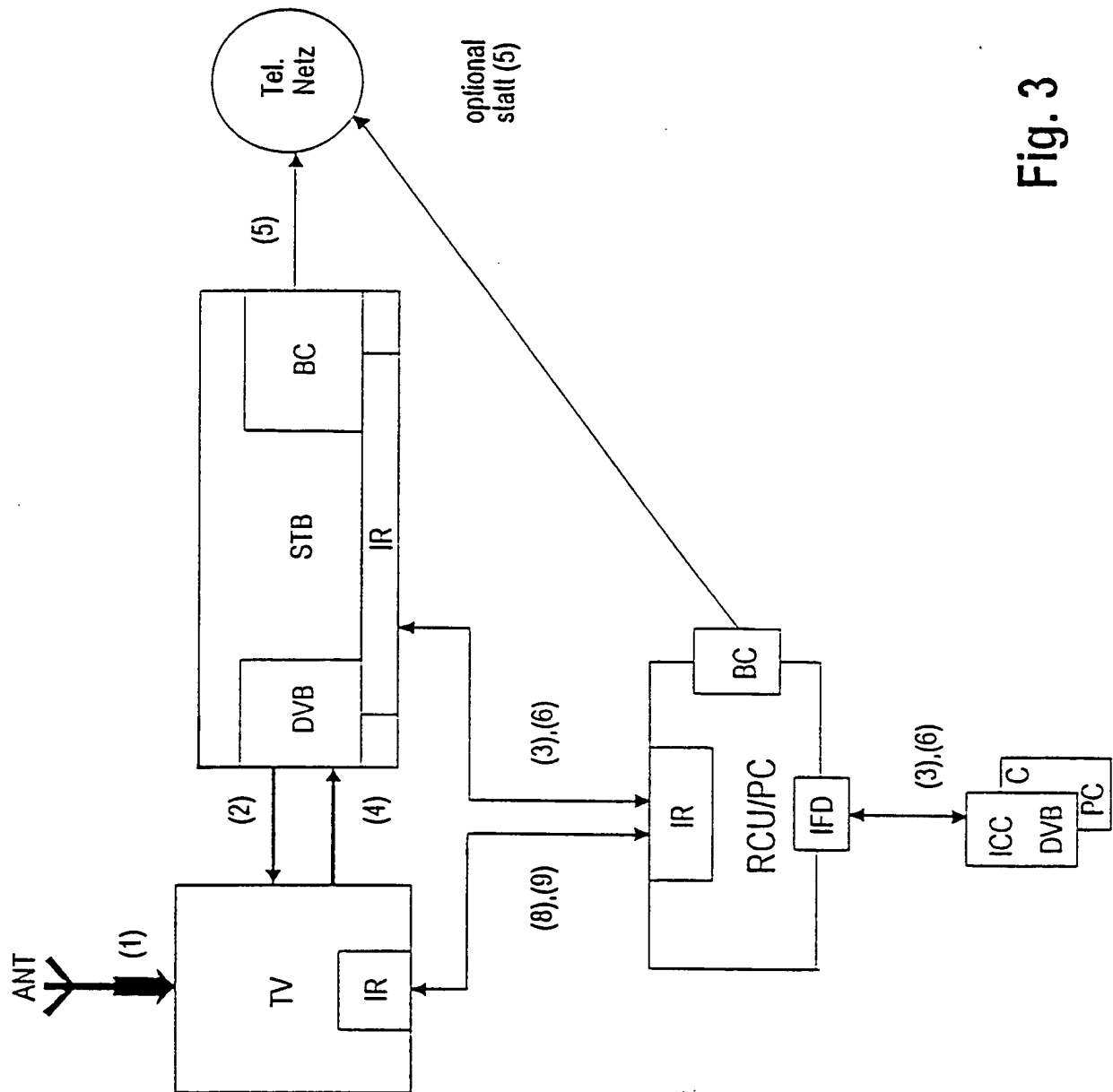


Fig. 3

**THIS PAGE BLANK (USPTO)**

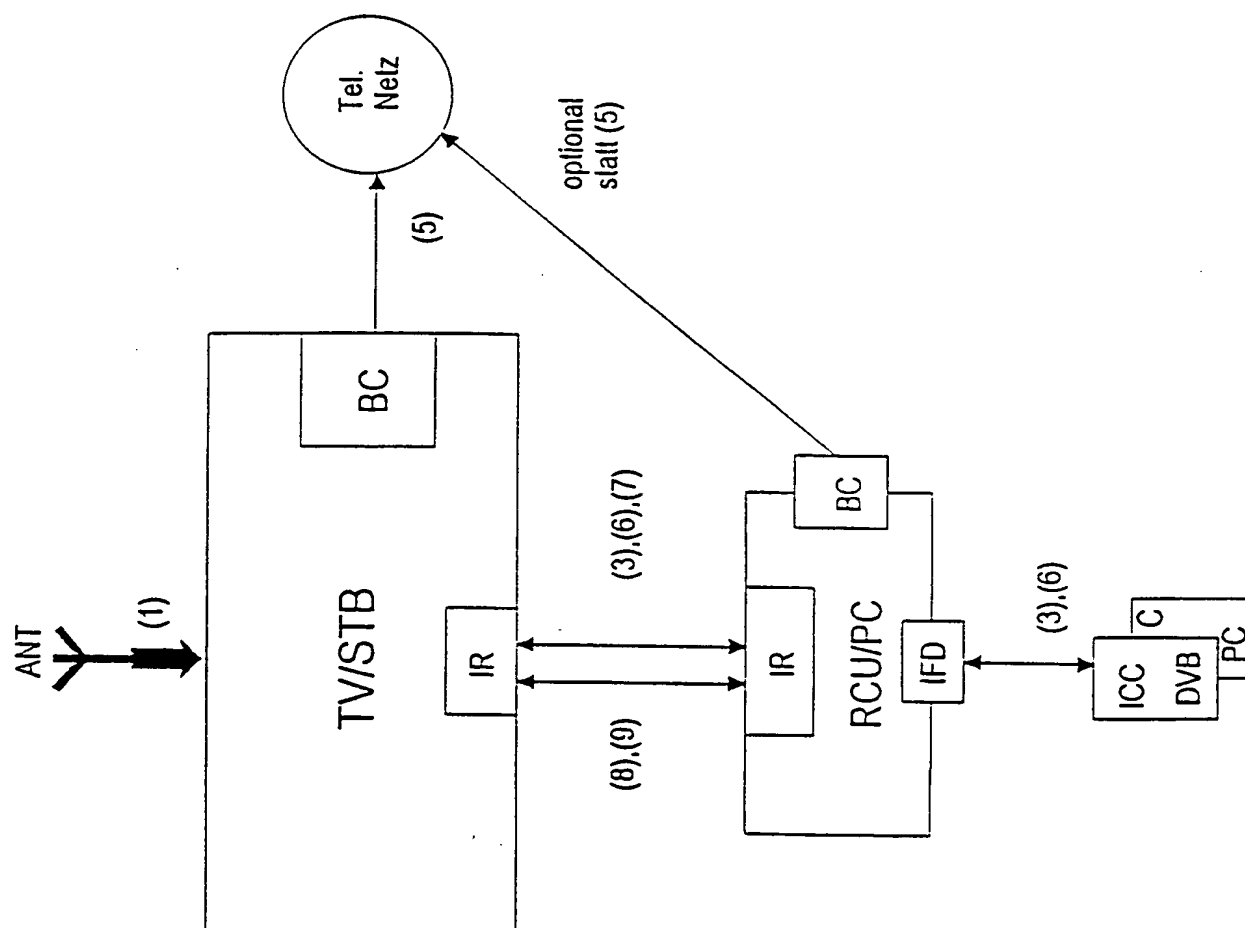


Fig. 4

**THIS PAGE BLANK (USPTO)**



# INTERNATIONAL SEARCH REPORT

International Application No

PCT/EP 98/04424

## A. CLASSIFICATION OF SUBJECT MATTER

IPC 6 H04N7/16

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 6 H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 97 20431 A (THOMSON MULTIMEDIA SA ; VITO MARIO DE (FR); GREGOIRE LOUIS (FR)) 5 June 1997 see page 5, line 27 - page 7, line 8 see page 12, line 1 - line 23 see page 16, line 24 - page 19, line 7 see figures 1,2,4 ---	1-14
Y	WO 96 32702 A (SMART TV CO) 17 October 1996 see page 4, line 11 - page 6, line 13 see page 8, line 9 - line 31 see figures 1-6 --- -/--	1-14

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

### \* Special categories of cited documents :

- "A" document defining the general state of the art which is not considered to be of particular relevance
- "E" earlier document but published on or after the international filing date
- "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- "O" document referring to an oral disclosure, use, exhibition or other means
- "P" document published prior to the international filing date but later than the priority date claimed

- "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- "&" document member of the same patent family

Date of the actual completion of the international search

16 November 1998

Date of mailing of the international search report

26/11/1998

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,  
Fax: (+31-70) 340-3016

Authorized officer

Van der Zaal, R

# INTERNATIONAL SEARCH REPORT

1st Application No

PCT/EP 98/04424

## C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	GB 2 304 217 A (GEN INFORMATION SYSTEMS LTD) 12 March 1997 see page 5, line 17 - page 7, line 2 see page 8, line 8 - line 13 see page 12, line 3 - page 13, line 14 see figures 2-4 ---	1-6,9
A	BUER M ET AL: "INTEGRATED SECURITY FOR DIGITAL VIDEO BROADCAST" IEEE TRANSACTIONS ON CONSUMER ELECTRONICS, vol. 42, no. 3, August 1996, pages 500-503, XP000638531 see page 501, left-hand column, line 6 - page 503, left-hand column, line 35 ---	10-14
A	DE 94 17 937 U (C.I.S. HOTEL COMMUNICATIONS GMBH) 27 April 1995 see page 6, line 21 - page 9, line 18 see figures 1-4 -----	1,2,6

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/EP 98/04424

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9720431 A	05-06-1997	FR 2741972 A EP 0864226 A	06-06-1997 16-09-1998
WO 9632702 A	17-10-1996	AU 5449796 A CA 2218067 A	30-10-1996 17-10-1996
GB 2304217 A	12-03-1997	AU 6706396 A WO 9707632 A	12-03-1997 27-02-1997
DE 9417937 U	16-03-1995	AT 169170 T DE 19520180 A DE 59503015 D WO 9615629 A EP 0791272 A	15-08-1998 15-05-1996 03-09-1998 23-05-1996 27-08-1997

**THIS PAGE BLANK (USPTO)**

5330  
09/485408

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT  
AUF DEM GEBIET DES PATENTWESENS

PCT

INTERNATIONALER RECHERCHENBERICHT

(Artikel 18 sowie Regeln 43 und 44 PCT)

Aktenzeichen des Anmelders oder Anwalts <b>P96198W0/EK03</b>	<b>WEITERES VORGEHEN</b> siehe Mitteilung über die Übermittlung des internationalen Recherchenberichts (Formblatt PCT/ISA/220) sowie, soweit zutreffend, nachstehender Punkt 5	
Internationales Aktenzeichen <b>PCT/EP 98/04424</b>	Internationales Anmeldedatum (Tag/Monat/Jahr) <b>16/07/1998</b>	(Frühestes) Prioritätsdatum (Tag/Monat/Jahr) <b>06/08/1997</b>
Anmelder  <b>DEUTSCHE TELEKOM AG et al.</b>		

Dieser internationale Recherchenbericht wurde von der Internationalen Recherchenbehörde erstellt und wird dem Anmelder gemäß Artikel 18 übermittelt. Eine Kopie wird dem Internationalen Büro übermittelt.

Dieser internationale Recherchenbericht umfaßt insgesamt 3 Blätter.

☒ Darüber hinaus liegt ihm jeweils eine Kopie der in diesem Bericht genannten Unterlagen zum Stand der Technik bei.

1. ☐ Bestimmte Ansprüche haben sich als nichtrecherchierbar erwiesen (siehe Feld I).
2. ☐ Mangelnde Einheitlichkeit der Erfindung (siehe Feld II).
3. ☐ In der internationalen Anmeldung ist ein Protokoll einer Nucleotid- und/oder Aminosäuresequenz offenbart; die internationale Recherche wurde auf der Grundlage des Sequenzprotokolls durchgeführt,
  - ☐ das zusammen mit der internationalen Anmeldung eingereicht wurde.
  - ☐ das vom Anmelder getrennt von der internationalen Anmeldung vorgelegt wurde,
    - ☐ dem jedoch keine Erklärung beigelegt war, daß der Inhalt des Protokolls nicht über den Offenbarungsgehalt der internationalen Anmeldung in der eingereichten Fassung hinausgeht.
  - ☐ das von der Internationalen Recherchenbehörde in die ordnungsgemäße Form übertragen wurde.
4. Hinsichtlich der Bezeichnung der Erfindung
  - ☒ wird der vom Anmelder eingereichte Wortlaut genehmigt.
  - ☐ wurde der Wortlaut von der Behörde wie folgt festgesetzt.
5. Hinsichtlich der Zusammenfassung
  - ☒ wird der vom Anmelder eingereichte Wortlaut genehmigt.
  - ☐ wurde der Wortlaut nach Regel 38.2b) in der Feld III angegebenen Fassung von dieser Behörde festgesetzt. Der Anmelder kann der Internationalen Recherchenbehörde innerhalb eines Monats nach dem Datum der Absendung dieses internationalen Recherchenberichts eine Stellungnahme vorlegen.
6. Folgende Abbildung der Zeichnungen ist mit der Zusammenfassung zu veröffentlichen:  
Abb. Nr. 2
  - ☒ wie vom Anmelder vorgeschlagen
  - ☐ weil der Anmelder selbst keine Abbildung vorgeschlagen hat.
  - ☐ weil diese Abbildung die Erfindung besser kennzeichnet.

☐ keine der Abb.

**THIS PAGE BLANK (USPTO)**

**A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES**

IPK 6 H04N7/16

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

**B. RECHERCHIERTE GEBIETE**

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)

IPK 6 H04N

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

**C. ALS WESENTLICH ANGESEHENE UNTERLAGEN**

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
Y	WO 97 20431 A (THOMSON MULTIMEDIA SA ; VITO MARIO DE (FR); GREGOIRE LOUIS (FR)) 5. Juni 1997 siehe Seite 5, Zeile 27 - Seite 7, Zeile 8 siehe Seite 12, Zeile 1 - Zeile 23 siehe Seite 16, Zeile 24 - Seite 19, Zeile 7 siehe Abbildungen 1,2,4 ---	1-14
Y	WO 96 32702 A (SMART TV CO) 17. Oktober 1996 siehe Seite 4, Zeile 11 - Seite 6, Zeile 13 siehe Seite 8, Zeile 9 - Zeile 31 siehe Abbildungen 1-6 --- -/--	1-14

☒ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen☒ Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :

"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden

"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

"&amp;" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche

16. November 1998

Absendedatum des internationalen Recherchenberichts

26/11/1998

Name und Postanschrift der Internationalen Recherchenbehörde  
Europäisches Patentamt, P.B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,  
Fax: (+31-70) 340-3016

Bevollmächtigter Bediensteter

Van der Zaal, R

**THIS PAGE BLANK (USPTO)**



## C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	GB 2 304 217 A (GEN INFORMATION SYSTEMS LTD) 12. März 1997 siehe Seite 5, Zeile 17 - Seite 7, Zeile 2 siehe Seite 8, Zeile 8 - Zeile 13 siehe Seite 12, Zeile 3 - Seite 13, Zeile 14 siehe Abbildungen 2-4 ----	1-6,9
A	BUER M ET AL: "INTEGRATED SECURITY FOR DIGITAL VIDEO BROADCAST" IEEE TRANSACTIONS ON CONSUMER ELECTRONICS, Bd. 42, Nr. 3, August 1996, Seiten 500-503, XP000638531 siehe Seite 501, linke Spalte, Zeile 6 - Seite 503, linke Spalte, Zeile 35 ----	10-14
A	DE 94 17 937 U (C.I.S. HOTEL COMMUNICATIONS GMBH) 27. April 1995 siehe Seite 6, Zeile 21 - Seite 9, Zeile 18 siehe Abbildungen 1-4 -----	1,2,6

**THIS PAGE BLANK (USPTO)**

# INTERNATIONALES RESEARCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen

PCT/EP 98/04424

Im Recherchenbericht angeführtes Patentdokument		Datum der Veröffentlichung	Mitglied(er) der Patentfamilie		Datum der Veröffentlichung
WO 9720431	A	05-06-1997	FR	2741972 A	06-06-1997
			EP	0864226 A	16-09-1998
WO 9632702	A	17-10-1996	AU	5449796 A	30-10-1996
			CA	2218067 A	17-10-1996
GB 2304217	A	12-03-1997	AU	6706396 A	12-03-1997
			WO	9707632 A	27-02-1997
DE 9417937	U	16-03-1995	AT	169170 T	15-08-1998
			DE	19520180 A	15-05-1996
			DE	59503015 D	03-09-1998
			WO	9615629 A	23-05-1996
			EP	0791272 A	27-08-1997

**THIS PAGE BLANK (USPTO)**